

200141196

General Information

Record Number:	200141196	**Center:**	JPL
Title:	10 RedHat Linux Systems Compromised at JPL		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	
Incident Category:	System Compromise	**Est. Cost ($):**	2400
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C sa.gov
		Source of Report:	b6, 7C
		Est. Cost (hours):	24

Incident Dates

Incident Date:	11/28/2003	**Incident Zone:**	PST
Discovered Date:	11/28/2003	**Discovered Zone:**	
NASIRC Notified Date:	12/1/2003	**NASIRC Notified Zone:**	EDT
Closed Date:	12/19/2003	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



~~SENSITIVE BUT UNCLASSIFIED~~

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(C), (b) (7)(E)			Redhat		Linux 7.1		Tool Builder		257				Linux ptrace() kmod	6302		N/A	
			Redhat		Linux 7.x				257				Linux ptrace() kmod	6313		N/A	
			Sun (Software)		Solaris 8				383				Local Root Exploit	6314		N/A	
			Sun (Software)		Solaris 8								Local Root Exploit	6316		N/A	
			Sun (Software)		Solaris 2.6								Linux ptrace() kmod	6317		N/A	
			Redhat		Linux 7.1		Workstation		257				Linux ptrace() kmod	6301		N/A	
			Redha		Linux				448				Linux	6312		N/	

(b) (6), (b) (7)(C), (b) (7)(E)	Sun (Software)	Solaris 2.5		11	Solaris priocntl() Local Root	6315	N/A
	Sun (Software)	Solaris 8			Local Root Exploit	6318	N/A
	Redhat	Linux 7.x	Workstation		Linux ptrace() kmod	6979	

Hostile Site Information

IP Address	hostile_site_id
b6, 7E	41509

Additional Information

Notices

All of the highlighted texts will be released

ID	Abbreviation	noticeid	Date
2003-PLESAAA	FedCIRC	3237	01-DEC-2003
A-03-468	NASIRC	3236	01-DEC-2003
LTOOL-ID115-12-2003	Center	3240	05-DEC-2003

Summary: 12/01/03: b(b6, 7C JPL reports the System Compromise of b6, 7E and b6, 7E Both systems are running RedHat Linux 7. Attacking IP not available at this time. NASIRC issued A-03-468. m. 12/02/2003: FedCIRIC #2003-PLESAAA added. (b6, 12/05/2003: Weekly update from JPL below. (b6, 12/18/2003: Update per b6, 7C , incident was reopened on their end due to more hosts being infected. (b6, 12/19/2003: Closed per b6, 7C incident closed. (b6,

Chronology: -----Original Message----- From: b6, 7C jpl.nasa.gov [mailto:b6, 7C jpl.nasa.gov] Sent: Monday, December 01, 2003 4:27 PM To: b2, 7E hq.nasa.gov; b6, 7C .jpl.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; b6, 7C .jpl.nasa.gov; b2, 7E hq.nasa.gov; b2, 7E jpl.nasa.gov Subject: (NASIRC Ref: b6, 7E) JPL Incident Initial Notification (ID_115) INITIAL INCIDENT NOTIFICATION Investigation Name:LTOOL-ID115-12-2003 Incident Date:2003-11-28, 17:45 Investigator Name:(b) (6), (b) (7)(C) Notified By:RealSecure JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. b6, 7E | b6, 7E | RedHat Linux 7.x | b6, 7E | SC | Undetermined | No | None 2. b6, 7E | b6, 7E | RedHat Linux 7.x | Workstation | SC | Undetermined | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ** FedCIRC has received your incident report, NASIRC A-03-468 and will process accordingly. Your incident has been assigned FedCIRC incident # 2003-PLESAAA for future reference. - - The automated FedCIRC Incident Report Form is available here: http://www.fedcirc.gov/reportform.html - - Additional information regarding FedCIRC and incident reporting/handling is available at the FedCIRC website (http://www.fedcirc.gov). Thank you, FedCIRC Operations Phone: b6, 7C Fax: 703-326-9461 email: fedcirc@fedcirc.gov ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:b6, 7C jpl.nasa.gov] Sent: Friday, December 05, 2003 2:36 PM To: b2, 7E hq.nasa.gov Cc: b2, 7E jpl.nasa.gov Subject: (NASIRC Ref: 107398094) Weekly Incident Report for 21Nov03_04Dec03 ** NEW INCIDENTS: 1 ** INCIDENT INFO Incident Name:b6, 7E ID115-12-2003 Discovery Date:28-NOV-03 Exploit Date:28-NOV-03 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:b6, 7E Hostile IP:b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:7.1 System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:7.1 System Security Plan:257 ******** (b) (6), (b) (7)(C) ****** -----Original Message----- From: b6, 7C [mailto (b) (6), (b) (7)(C) nasa.gov] Sent: Thursday, December 18, 2003 10:58 AM To: b2, 7E hq.nasa.gov; b6, 7C b6, 7C jpl.nasa.gov Subject: (NASIRC Ref: 107398850) Re: (Low:N/A N/A) Morning Read Board [NASIRC H-03-62] JPL: >1 incident, 2 systems: 200141196 b6, jpl.nasa.gov b6, 7E > b6, 7E .jpl.nasa.gov (b6, 7E This has been reopened as we found a few more hosts infected - most have been cleaned up. Linux machines - ptrace and do_brk kernel exploits, along with ettercap sniffers ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:b6, 7C jpl.nasa.gov] Sent: Thursday, December 18, 2003 7:24 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107399025) Weekly Incident Report for 05Dec03_17Dec03 ** ****** NEW INCIDENTS: 0 ** OPEN INCIDENTS: 1 ** INCIDENT INFO Incident Name:LTOOL-ID115-12-2003 Discovery Date:28-NOV-03 Exploit Date:28-NOV-03 Labor Hours:24 Labor Cost:$2400 HOSTILE SYSTEMS Hostile Name:b6, 7E Hostile IP:b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:n/a Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:448 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:7.1 System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:383 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:383 Domain Name:b6, 7E JPL.jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.5 (5.5) OS Version:n/a System Security Plan:11 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:Trojan Exploit Used:Local Ptrace Root Exploit System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:n/a Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:7.1 System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:n/a --- ** CLOSED INCIDENTS: 1 ** INCIDENT INFO Incident Name:b6, 7E ID115-12-2003 Discovery Date:28-NOV-03 Exploit Date:28-NOV-03 Labor Hours:24 Labor Cost:2400



HOSTILE SYSTEMS Hostile Name:b6, 7E Hostile IP:b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:n/a Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:448 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS: RedHat Linux 7.x OS Version:7.1 System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:383 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:383 Domain Name:b6, 7E JPL.jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:b6, 7E Local Root System OS:Sun Solaris 2.5 (5.5) OS Version:n/a System Security Plan:11 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:Trojan Exploit Used:Local Ptrace Root Exploit System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:n/a Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Ptrace Root Exploit System OS:RedHat Linux 7.x OS Version:7.1 System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:n/a

NASIRC Notes:	



200141220

General Information

Record Number:	200141220	**Center:**	JPL
Title:	System Compromises at JPL via Yahoo Messenger		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	
Incident Category:	System Compromise	**Est. Cost ($):**	2800
Attacker:	Stakkato/stkto	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C .nasa.gov
		Source of Report:	b6, 7C
		Est. Cost (hours):	28

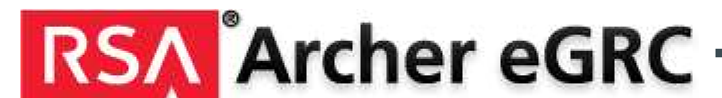
Incident Dates

Incident Date:	1/5/2004	**Incident Zone:**	PST
Discovered Date:	1/6/2004	**Discovered Zone:**	
NASIRC Notified Date:	1/8/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	2/17/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
b6, 7E			Microsoft	Microsoft	Windows 2000	Unknown	Workstation						Yahoo Messenger_YAuto.dll BO	6339		ADM	
b6, 7E			Microsoft	Microsoft	Windows 2000	Unknown	Workstation						Yahoo Messenger_YAuto.dll BO	6340		ADM	

Hostile Site Information

IP Address	hostile_site_id
b6, 7E	41526

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-09	NASIRC	3248	08-JAN-2004
A-04-09-A	NASIRC	3286	14-FEB-2004

RSA Archer eGRC

CTRINH-PC-ID118-01-2	Center	3247	08-JAN-2004

Summary: 02/17/2004: Closed incident per Weekly update from b6, 7C @ JPL. (b) (6), (b

Chronology: -----Original Message----- From: (b) (6), (b) (7)(C) nasa.gov [mailto:(b) (6), (b) (7)(C) nasa.gov] Sent: Thursday, January 08, 2004 3:51 PM To: jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107400475) JPL Incident Initial Notification (ID_118) INITIAL INCIDENT NOTIFICATION Investigation Name:CTRINH-PC-ID118-01-2004 Incident Date:2004-01-05, 00:00 Investigator Name:b6, 7C Notified By:JPL User JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | b6, 7E | MS Windows 2000 | workstation | SC | Yahoo! Messenger YAUTO.DLL | No | None 2. b6, 7E 9 | b6, 7E | MS Windows 2000 | workstation | SC | Yahoo! Messenger YAUTO.DLL | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY b6, 7E | St Louis | MD | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:b6, 7C jpl.nasa.gov] Sent: Friday, February 13, 2004 5:31 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107404671) Weekly Incident Report for 06Feb04_12Feb04 ** CLOSED INCIDENTS: 3 ** INCIDENT INFO Incident Name:CTRINH-PC-ID118-01-2004 Discovery Date:06-JAN-04 Exploit Date:05-JAN-04 Labor Hours:28 Labor Cost:2800 HOSTILE SYSTEMS Hostile Name b6, 7E Hostile IP:b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Yahoo! Messenger YAUTO.DLL System OS:MS Windows 2000 OS Version:w2k System Security Plan:n/a Domain Name:b6, 7E .jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Yahoo! Messenger YAUTO.DLL System OS:MS Windows 2000 OS Version:2k System Security Plan:n/a -- INCIDENT INFO Incident Name:b6, 7E -ID120-01-2004 Discovery Date:10-JAN-04 Exploit Date:07-JAN-04 Labor Hours:92 Labor Cost:9200 HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E .jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 7.x OS Version:- System Security Plan:123 Domain Name:b6, 7E .jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 7.x OS Version:- System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:257 Domain Name:b6, jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name:b6, 7C jpl.nasa.gov IP Address:b6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:HP-UX 9.x & 10.x OS Version:- System Security Plan:257 Domain Name:b6, jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 7.x OS Version:- System Security Plan:257 Domain Name:b6, jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:11 -- INCIDENT INFO Incident Name:b6, 7E ID125-02-2004 Discovery Date:10-FEB-04 Exploit Date:07-FEB-04 Labor Hours:8 Labor Cost:800 HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:b6, 7E Hostile Name:(b) (6), (b) (7)(E) Hostile IP:b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:503 --

NASIRC Notes:



200141221

General Information

Record Number:	200141221	**Center:**	JPL
Title:	System Compromises at JPL via Local Root Exploit		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	b6, 7C
Incident Category:	System Compromise	**Est. Cost ($):**	4600
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C .nasa.gov
		Source of Report:	b6, 7C
		Est. Cost (hours):	46

Incident Dates

Incident Date:	1/7/2004	**Incident Zone:**	
Discovered Date:	1/10/2004	**Discovered Zone:**	
NASIRC Notified Date:	1/12/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	2/17/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
b6, 7C			Sun (Software)		Solaris 9				370				Local Root Exploit	6344			
b6, 7C			Sun (Software)		Solaris 9				370				Local Root Exploit	6346			
b6, 7C			Sun (Software)		Solaris 9				370				Local Root Exploit	6342			
b6, 7C			Redhat		Linux 7.x		Workstation		257				Local Root Exploit	6341		N/A	
b6, 7C			Redhat		Linux 7.x		Workstation		123				Local Root Exploit	6978			
b6, 7C			Sun (Software)		Solaris 9				11				Local Root Exploit	6996			

Hostile Site Information



IP Address	hostile_site_id
b6, 7C	41905

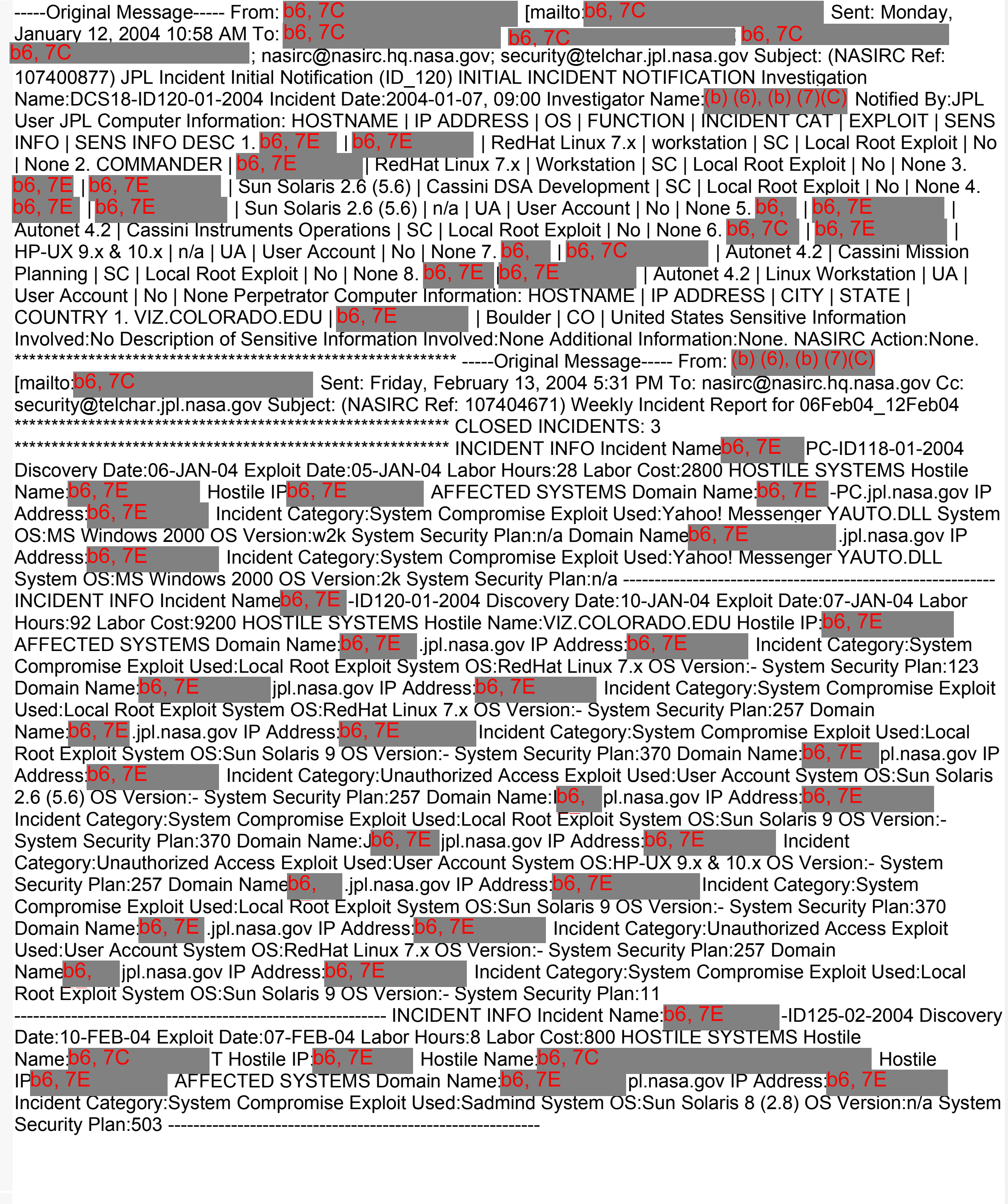
Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-12	NASIRC	3252	12-JAN-2004
DCS18-IDI20-01-2004	Center	3251	12-JAN-2004

Summary: 02/17/2004: Incident closed per weekly report from b6, 7C at JPL. (b) (6), (b 02/17/2004: Per b6, 7C (b) (6), (b divided the cost in 1/2 for 200141221 & 200141224. JPL s database reflects this as 1 incident, for reporting purposes NASIRC seperated the system compromises & unauthorized accesses into 2 incidents. Total cost is $9200 each incident now reflects a cost of $4600. b6,

Chronology:



-----Original Message----- From: b6, 7C [mailto:b6, 7C Sent: Monday, January 12, 2004 10:58 AM To: b6, 7C b6, 7C b6, 7C b6, 7C ; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107400877) JPL Incident Initial Notification (ID_120) INITIAL INCIDENT NOTIFICATION Investigation Name:DCS18-ID120-01-2004 Incident Date:2004-01-07, 09:00 Investigator Name:(b) (6), (b) (7)(C) Notified By:JPL User JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. b6, 7E | b6, 7E | RedHat Linux 7.x | workstation | SC | Local Root Exploit | No | None 2. COMMANDER | b6, 7E | RedHat Linux 7.x | Workstation | SC | Local Root Exploit | No | None 3. b6, 7E | b6, 7E | Sun Solaris 2.6 (5.6) | Cassini DSA Development | SC | Local Root Exploit | No | None 4. b6, 7E | b6, 7E | Sun Solaris 2.6 (5.6) | n/a | UA | User Account | No | None 5. b6, | b6, 7E | Autonet 4.2 | Cassini Instruments Operations | SC | Local Root Exploit | No | None 6. b6, 7C | b6, 7E | HP-UX 9.x & 10.x | n/a | UA | User Account | No | None 7. b6, | b6, 7C | Autonet 4.2 | Cassini Mission Planning | SC | Local Root Exploit | No | None 8. b6, 7E | b6, 7E | Autonet 4.2 | Linux Workstation | UA | User Account | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. VIZ.COLORADO.EDU | b6, 7E | Boulder | CO | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:b6, 7C Sent: Friday, February 13, 2004 5:31 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107404671) Weekly Incident Report for 06Feb04_12Feb04 ** CLOSED INCIDENTS: 3 ** INCIDENT INFO Incident Nameb6, 7E PC-ID118-01-2004 Discovery Date:06-JAN-04 Exploit Date:05-JAN-04 Labor Hours:28 Labor Cost:2800 HOSTILE SYSTEMS Hostile Name:b6, 7E Hostile IPb6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E -PC.jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Yahoo! Messenger YAUTO.DLL System OS:MS Windows 2000 OS Version:w2k System Security Plan:n/a Domain Nameb6, 7E .jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Yahoo! Messenger YAUTO.DLL System OS:MS Windows 2000 OS Version:2k System Security Plan:n/a -- INCIDENT INFO Incident Nameb6, 7E -ID120-01-2004 Discovery Date:10-JAN-04 Exploit Date:07-JAN-04 Labor Hours:92 Labor Cost:9200 HOSTILE SYSTEMS Hostile Name:VIZ.COLORADO.EDU Hostile IP:b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E .jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 7.x OS Version:- System Security Plan:123 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 7.x OS Version:- System Security Plan:257 Domain Name:b6, 7E .jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name:b6, 7E pl.nasa.gov IP Address:b6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:257 Domain Name:b6, pl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name:Jb6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:HP-UX 9.x & 10.x OS Version:- System Security Plan:257 Domain Nameb6, .jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name:b6, 7E .jpl.nasa.gov IP Address:b6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 7.x OS Version:- System Security Plan:257 Domain Nameb6, jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:11 -- INCIDENT INFO Incident Name:b6, 7E -ID125-02-2004 Discovery Date:10-FEB-04 Exploit Date:07-FEB-04 Labor Hours:8 Labor Cost:800 HOSTILE SYSTEMS Hostile Name:b6, 7C T Hostile IP:b6, 7E Hostile Name:b6, 7C Hostile IPb6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E pl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:503 --

NASIRC Notes:



200141224

General Information

Record Number:	200141224	**Center:**	JPL
Title:	Unauthorized Access at JPL via user account		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	4600
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C)
		Source of Report:	b6, 7C
		Est. Cost (hours):	46

Incident Dates

Incident Date:	1/7/2004	**Incident Zone:**	
Discovered Date:	1/10/2004	**Discovered Zone:**	
NASIRC Notified Date:	1/14/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	2/17/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Redhat		Linux 7.x				257				Account - User	6347			
			Hewlett Packard		HP-UX				257				Account - User	6345			
			Sun (Software)		Solaris 2.6				257				Account - User	6343		N/A	

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41906

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-12	NASIRC	3254	12-JAN-2004
DCS18-ID120-01-2004	Center	3253	12-JAN-2004

Summary: 02/17/2004: Incident closed per weekly update provided my (b) (6), (b) (7)(C) @ JPL. ((b) (6), (b) 02/17/2004: Per (b) (6), (b) (7)(C) (b) (6), (b) (7)(C), (b) (6), (b) divided the cost in 1/2 for 200141221 & 200141224. JPL s database reflects this as 1 incident, for 7C reporting purposes NASIRC seperated the system compromises & unauthorized accesses into 2 incidents. Total cost is $9200 each incident now reflects a cost of $4600. ((b) (6), (b)

Chronology: -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C) Sent: Monday, January 12, 2004 10:58 AM To: b6, 7C (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) v; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107400877) JPL Incident Initial Notification (ID_120) INITIAL INCIDENT NOTIFICATION Investigation Name:(b) (6), (b) (7)(E)-ID120-01-2004 Incident Date:2004-01-07, 09:00 Investigator Name:(b) (6), (b) (7)(C) Notified By:JPL User JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 7.x | workstation | SC | Local Root Exploit | No | None 2. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 7.x | Workstation | SC | Local Root Exploit | No | None 3. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 2.6 (5.6) | Cassini DSA Development | SC | Local Root Exploit | No | None 4. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 2.6 (5.6) | n/a | UA | User Account | No | None 5. (b) (6), (b) | (b) (6), (b) (7)(E) | Autonet 4.2 | Cassini Instruments Operations | SC | Local Root Exploit | No | None 6. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | HP-UX 9.x & 10.x | n/a | UA | User Account | No | None 7. (b) (6), (b) (7) | (b) (6), (b) (7)(E) | Autonet 4.2 | Cassini Mission Planning | SC | Local Root Exploit | No | None 8. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Autonet 4.2 | Linux Workstation | UA | User Account | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Boulder | CO | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C) Sent: Friday, February 13, 2004 5:31 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107404671) Weekly Incident Report for 06Feb04_12Feb04 ** CLOSED INCIDENTS: 3 ** INCIDENT INFO Incident Name:(b) (6), (b) (7)(E)-PC-ID118-01-2004 Discovery Date:06-JAN-04 Exploit Date:05-JAN-04 Labor Hours:28 Labor Cost:2800 HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name(b) (6), (b) (7)(E) IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Yahoo! Messenger YAUTO.DLL System OS:MS Windows 2000 OS Version:w2k System Security Plan:n/a Domain Name(b) (6), (b) (7)(E).nasa.gov IP Address(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Yahoo! Messenger YAUTO.DLL System OS:MS Windows 2000 OS Version:2k System Security Plan:n/a -- INCIDENT INFO Incident Name:DCS18-ID120-01-2004 Discovery Date:10-JAN-04 Exploit Date:07-JAN-04 Labor Hours:92 Labor Cost:9200 HOSTILE SYSTEMS Hostile Name:VIZ.COLORADO.EDU Hostile IP:b6, 7C AFFECTED SYSTEMS Domain Name(b) (6), (b) (7)(E) IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 7.x OS Version:- System Security Plan:123 Domain Name:(b) (6), (b) (7)(E).nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 7.x OS Version:- System Security Plan:257 Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:257 Domain Name(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E).nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:HP-UX 9.x & 10.x OS Version:- System Security Plan:257 Domain Name(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:370 Domain Name(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 7.x OS Version:- System Security Plan:257 Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 9 OS Version:- System Security Plan:11 -- INCIDENT INFO Incident Name:(b) (6), (b) (7)(E) Discovery Date:10-FEB-04 Exploit Date:07-FEB-04 Labor Hours:8 Labor Cost:800 HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) Hostile Name:(b) (6), (b) (7)(E) Hostile IP(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name(b) (6), (b) (7)(E).nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:503 --

NASIRC Notes:



200141238

General Information

Record Number:	200141238	**Center:**	JPL
Title:	System compromises at JPL (16)		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	b6, 7C
Incident Category:	System Compromise	**Est. Cost ($):**	10275
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C .nasa.gov
		Source of Report:	b6, 7C
		Est. Cost (hours):	102.75

Incident Dates

Incident Date:	2/11/2004	**Incident Zone:**	
Discovered Date:	2/11/2004	**Discovered Zone:**	
NASIRC Notified Date:	2/12/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	3/22/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
b6, 7E			Sun (Software)		Solaris 2.6				370				Solaris priocntl() Local Root	7023			
b6, 7E			Sun (Software)		Solaris 8								Local Root Exploit	7224		N/A	
b6, 7E			Sun (Software)		Solaris 7				370					7011			
b6, 7E			Sun (Software)		Solaris 7				149				Password - Compromised	7012			
b6, 7E			Sun (Software)		Solaris 7				370				Solaris priocntl() Local Root	7013			
b6, 7E			Redha		Linux								Undet	7014			

b6, 7E	Redhat	Linux 7.x	149	Password - Compromised	7015
b6, 7E	Hewlet Packard	HP-UX	257	Undetermined	7016
b6, 7E	SGI	IRIX 6.5	149	Password - Compromised	7017
b6, 7E	Sun (Software)	Solaris 2.6	370	Solaris priocnt 1() Local Root	7018
b6, 7E	Sun (Software)	Solaris 8	100	Undetermined	7019
b6, 7E	Sun (Software)	Solaris 7	370	Solaris priocnt 1() Local Root	7021
b6, 7E	Sun (Software)	Solaris 2.6	370	Solaris priocnt 1() Local Root	7022
b6, 7E	Sun (Software)	Solaris 8	100	Undetermined	7020
b6, 7E	Sun (Software)	Solaris 8	257	SolSadmindAmslverifyBo	6990
b6, 7E	Sun (Softw are)	Solaris 8		SolSadmind Amslv	6991



Hostile Site Information

IP Address	hostile_site_id
b6, 7E	41910

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-44	NASIRC	3274	12-FEB-2004
A-04-44-A	NASIRC	3275	23-FEB-2004
SSD-ID127-02-2004	Center	3265	12-FEB-2004

Summary: 02/23/2004: 13 additional systems added per weekly incident report for 13Feb04-19Feb04 provided by b6, b6, ((b) (6), (b 03/15/2004: Incident closed per weekly report provided by b6, 7C (b) (6), (b 03/22/2004: Cost & labor were provided as 137 hours and $13,700 total cost. I put 3/4 of the labor and cost to this incident "System Compromise" the other 1/4 $3,425.00 to incident 200141246 "Unauthorized access at JPL". b6,

Chronology: -----Original Message----- From: b6, 7C [mailto:b6, 7C Sent: Wednesday, February 11, 2004 7:40 PM To: b6, 7C ; b6, 7C ; b6, 7C b6, 7C nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107404420) JPL Incident Initial Notification (ID_127) INITIAL INCIDENT NOTIFICATION Investigation Name:SSD-ID127-02-2004 Incident Date:2004-02-11, 04:30 Investigator Name:(b) (6), (b) (7)(C) Notified By:RealSecure JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. SSD | b6, 7E | Sun Solaris 8 (2.8) | Horizons Server | SC | Sadmind | No | None 2. TOMTOM | b6, 7E | Sun Solaris 8 (2.8) | server | SC | Sadmind | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. CELICA.CALTECH.EDU | 131.215.159.69 | Pasadena | CA | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. *** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:b6, 7C Sent: Friday, February 20, 2004 4:59 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107405286) Weekly Incident Report for 13Feb04_19Feb04 INCIDENT INFO Incident Name:SSD-ID127-02-2004 Discovery Date:11-FEB-04 Exploit Date:11-FEB-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:b6, 7E U Hostile IP:b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E pl.nasa.gov IP Address:b6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:SGI IRIX 6.5.x OS Version:- System Security Plan:0 Domain Nameb6, 7E .jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Nameb6, 7E .jpl.nasa.gov IP Addressb6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Nameb6, 7E .jpl.nasa.gov IP Addressb6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:100 Domain Name:b6, 7E jpl.nasa.gov IP Addressb6, 7E Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:100 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Root account cracked System OS:SGI IRIX 6.5.x OS Version:- System Security Plan:149 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Undetermined System OS:HP-UX 9.x & 10.x OS Version:- System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 7.x OS Version:- System Security Plan :149 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Undetermined System OS:RedHat Linux 9.x OS Version:- System Security Plan:n/a Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:149 Domain Name:b6, jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:n/a Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 *** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:b6, 7C Sent: Friday, March 12, 2004 5:13 PM To: nasirc@nasirc.hq.nasa.gov Cc: 7C security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107408126) Weekly Incident Report for 05Mar04_11Mar04 *** NEW INCIDENTS: 0 *** OPEN INCIDENTS: 0 *** CLOSED INCIDENTS: 4 *** INCIDENT INFO Incident Name:SSD-ID127-02-2004 Discovery Date:11-FEB-04 Exploit Date:11-FEB-04 Labor Hours:n/a Labor Cost: HOSTILE SYSTEMS Hostile Name:b6, 7E Hostile b6, 7E AFFECTED SYSTEMS Domain Name:b6, 7E .jpl.nasa.gov IP Addressb6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:SGI IRIX 6.5.x OS Version:- System Security Plan:0 Domain Name:b6, 7E .jpl.nasa.gov IP Addressb6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) b6, 7E 128.149.147.39 Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris

priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:100 Domain Name:b6, 7E jpl.nasa.gov IP Addressb6, 7E Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:0 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:100 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Sol aris 2.6 (5.6) OS Ver sion:- System Security Plan:370 Domain Name:b6, 7E nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:274 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Root account cracked System OS:SGI IRIX 6.5.x OS Version:- System Security Plan:149 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Undetermined System OS:HP-UX 9.x & 10.x OS Version:- System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 7.x OS Version:- System Security Plan:149 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Undetermined System OS:RedHat Linux 9.x OS Version:- System Security Plan:0 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:149 Domain Name:b6, jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:257 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:0 Domain Name:b6, 7E jpl.nasa.gov IP Address:b6, 7E Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:b6, 7C Sent: Monday, March 22, 2004 5:14 PM To: b6, 7C Subject: RE: (NASIRC Ref: 107409157) Weekly Incident Report for 12Mar04_19 Mar04 Hi b6, Update to close out JPL incident. SSD-ID127-02-2004 Labor Hours:137 Labor Cost:$13,700 b6,

NASIRC Notes:	



200141242

General Information

Record Number:	200141242	**Center:**	JPL
Title:	Unauthorized Access to (b) (6), (b) (7) jpl.nasa.gov ((b) (6), (b) (7)(E)) via user account		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	b6, 7C
Incident Category:	Unauthorized Access	**Est. Cost ($):**	300
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C .nasa.gov
		Source of Report:	b6, 7C
		Est. Cost (hours):	3

Incident Dates

Incident Date:	2/17/2004	**Incident Zone:**	
Discovered Date:	2/19/2004	**Discovered Zone:**	
NASIRC Notified Date:	2/19/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	3/15/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



SENSITIVE BUT UNCLASSIFIED

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Software)		Solaris 9				153				Account - User	7007		N/A	

Hostile Site Information

IP Address	hostile_site_id
(b) (7)(E), (b) (6)	41552
	41553

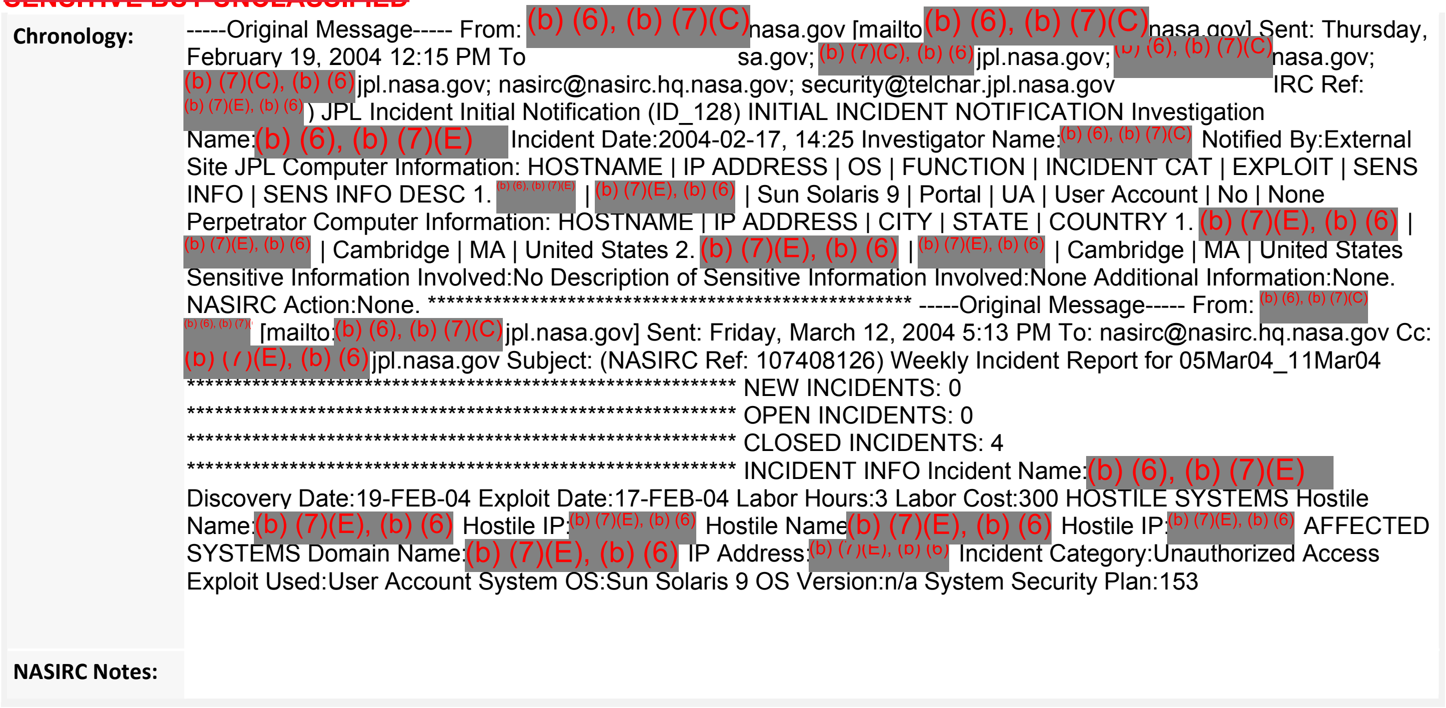
Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-50	NASIRC	3283	19-FEB-2004
(b) (6), (b) (7)(E)	Center	3267	19-FEB-2004

Summary: 03/15/2004: Closed incident per weekly report provided by b6, 7C (b)





Chronology:	-----Original Message----- From: (b) (6), (b) (7)(C) nasa.gov [mailto (b) (6), (b) (7)(C) nasa.gov] Sent: Thursday, February 19, 2004 12:15 PM To sa.gov; (b) (7)(C), (b) (6) jpl.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (7)(C), (b) (6) jpl.nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov IRC Ref: (b) (7)(E), (b) (6)) JPL Incident Initial Notification (ID_128) INITIAL INCIDENT NOTIFICATION Investigation Name: (b) (6), (b) (7)(E) Incident Date:2004-02-17, 14:25 Investigator Name: (b) (6), (b) (7)(C) Notified By:External Site JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | (b) (7)(E), (b) (6) | Sun Solaris 9 | Portal | UA | User Account | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. (b) (7)(E), (b) (6) | (b) (7)(E), (b) (6) | Cambridge | MA | United States 2. (b) (7)(E), (b) (6) | (b) (7)(E), (b) (6) | Cambridge | MA | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ** -----Original Message----- From: (b) (6), (b) (7)(C) (b) (6), (b) (7)([mailto: (b) (6), (b) (7)(C) jpl.nasa.gov] Sent: Friday, March 12, 2004 5:13 PM To: nasirc@nasirc.hq.nasa.gov Cc: (b) (7)(E), (b) (6) jpl.nasa.gov Subject: (NASIRC Ref: 107408126) Weekly Incident Report for 05Mar04_11Mar04 *** NEW INCIDENTS: 0 *** OPEN INCIDENTS: 0 *** CLOSED INCIDENTS: 4 *** INCIDENT INFO Incident Name: (b) (6), (b) (7)(E) Discovery Date:19-FEB-04 Exploit Date:17-FEB-04 Labor Hours:3 Labor Cost:300 HOSTILE SYSTEMS Hostile Name: (b) (7)(E), (b) (6) Hostile IP: (b) (7)(E), (b) (6) Hostile Name (b) (7)(E), (b) (6) Hostile IP: (b) (7)(E), (b) (6) AFFECTED SYSTEMS Domain Name: (b) (7)(E), (b) (6) IP Address: (b) (7)(E), (b) (6) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 9 OS Version:n/a System Security Plan:153
NASIRC Notes:	



200141246

General Information

Record Number:	200141246	**Center:**	JPL
Title:	Unauthorized Access at JPL		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	3425
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C).nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	34.25

Incident Dates

Incident Date:	2/11/2004	**Incident Zone:**	
Discovered Date:	2/11/2004	**Discovered Zone:**	
NASIRC Notified Date:	2/23/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	3/22/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info ?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Software)		Solaris 8								Account - User	7225		N/A	
			SGI		IRIX 6.5								Account - User	7010			

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41911

Additional Information

Notices

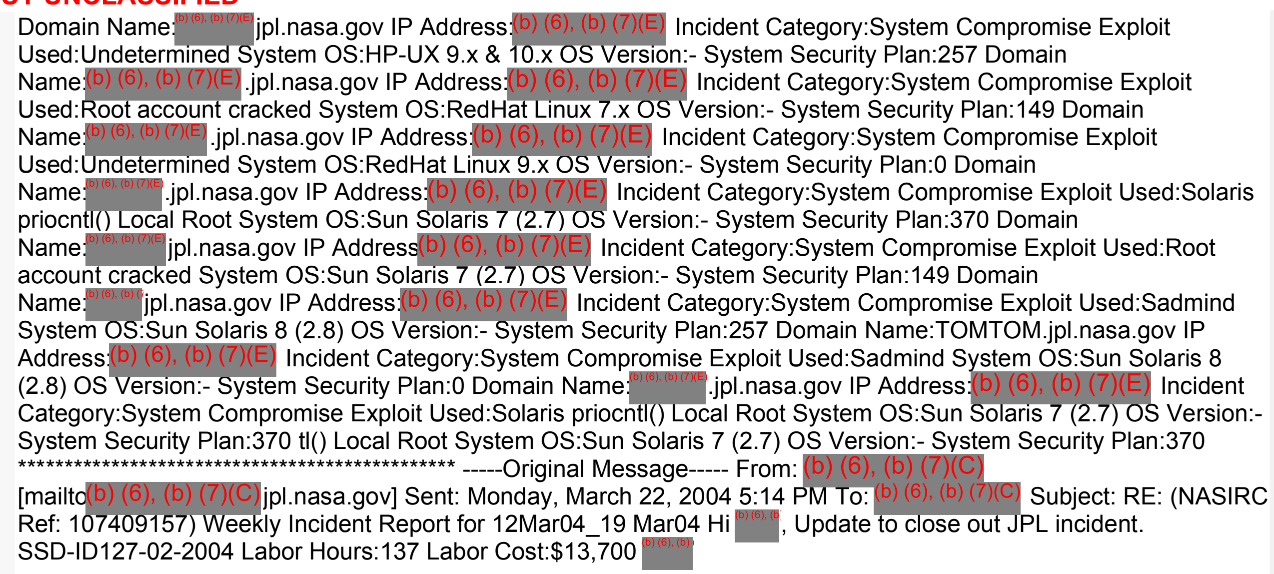
ID	Abbreviation	noticeid	Date
A-04-44-A	NASIRC	3282	23-FEB-2004
ssd-id127-02-2004	Center	3268	11-FEB-2004

Summary: 02/23/2004: Incident added per weekly incident report for 13Feb04-19Feb04 provided by (b) (6), (b) (7)(C) . (b) (6), (b) 03/15/2004: Closed incident per weekly report provided by (b) (6), (b) (7)(C) (b)(b) (6), (b) 03/22/2004: Cost & labor were provided as 137 hours and $13,700 total cost. I put 1/4 of the labor and cost to this incident "Unauthorized Access" the other 3/4 $10,750.00 to incident 200141238 "System Compromise". (b) (6), (b)

SENSITIVE BUT UNCLASSIFIED

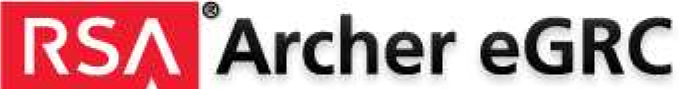
Chronology: -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C)jpl.nasa.gov] Sent: Friday, February 20, 2004 4:59 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107405286) Weekly Incident Report for 13Feb04_19Feb04 INCIDENT INFO Incident Name:SSD-ID127-02-2004 Discovery Date:11-FEB-04 Exploit Date:11-FEB-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:CELICA.CALTECH.EDU Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:SGI IRIX 6.5.x OS Version:- System Security Plan:0 Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:100 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:100 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Name(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:SGI IRIX 6.5.x OS Version:- System Security Plan:149 Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:HP-UX 9.x & 10.x OS Version:- System Security Plan:257 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 7.x OS Version:- System Security Plan:149 Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:RedHat Linux 9.x OS Version:- System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:149 Domain Name:(b) (6), (b).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E)Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:257 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocn ****************************** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C)jpl.nasa.gov] Sent: Friday, March 12, 2004 5:13 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107408126) Weekly Incident Report for 05Mar04_11Mar04 ** NEW INCIDENTS: 0 ** OPEN INCIDENTS: 0 ** CLOSED INCIDENTS: 4 ** INCIDENT INFO Incident Name:SSD-ID127-02-2004 Discovery Date:11-FEB-04 Exploit Date:11-FEB-04 Labor Hours:n/a Labor Cost: HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E)AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:SGI IRIX 6.5.x OS Version:- System Security Plan:0 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:100 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E)Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:0 Domain Name:(b) (6), (b) (7)(E)pl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:100 Domain Name:(b) (6), (b) (7)(E)pl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 2.6 (5.6) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:274 Domain Name(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:SGI IRIX 6.5.x OS Version:- System Security Plan:149





Domain Name:(b) (6), (b) (7)(E) jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:HP-UX 9.x & 10.x OS Version:- System Security Plan:257 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 7.x OS Version:- System Security Plan:149 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:RedHat Linux 9.x OS Version:- System Security Plan:0 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 Domain Name:(b) (6), (b) (7)(E) jpl.nasa.gov IP Address(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:149 Domain Name:(b) (6), (b) (jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:257 Domain Name:TOMTOM.jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Sadmind System OS:Sun Solaris 8 (2.8) OS Version:- System Security Plan:0 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Solaris priocntl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 tl() Local Root System OS:Sun Solaris 7 (2.7) OS Version:- System Security Plan:370 ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto(b) (6), (b) (7)(C) jpl.nasa.gov] Sent: Monday, March 22, 2004 5:14 PM To: (b) (6), (b) (7)(C) Subject: RE: (NASIRC Ref: 107409157) Weekly Incident Report for 12Mar04_19 Mar04 Hi (b) (6), (b , Update to close out JPL incident. SSD-ID127-02-2004 Labor Hours:137 Labor Cost:$13,700 (b) (6), (b)

NASIRC Notes:	



200141247

General Information

Record Number:	200141247	**Center:**	LaRC
Title:	SADMIND compromise - 23 hosts involved		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	LaRC	**Coordinator:**	b6, 7C
Incident Category:	System Compromise	**Est. Cost ($):**	88500
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C nasa.gov
		Source of Report:	
		Est. Cost (hours):	885

Incident Dates

Incident Date:	1/25/2004	**Incident Zone:**	EST
Discovered Date:	1/27/2004	**Discovered Zone:**	EST
NASIRC Notified Date:	1/27/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	2/25/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	1/27/2004	**ITSM Zone:**	EST
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Software)	Sun (Hardware)	Solaris								SolSadmindAmslverifyBo	7043		SER	
			Sun (Software)	Sun (Hardware)	Solaris								SolSadmindAmslverifyBo	7044		SER	
			Sun (Software)	Sun (Hardware)	Solaris								Undetermined	7045		PUB	
			Sun (Software)	Sun (Hardware)	Solaris								Password - Compromised	7038		SER	
			Sun (Software)	Sun (Hardware)	Solaris	Enterprise 250							Password - Compromised	7046		SER	
			Sun	Sun	Solaris								SolSa	7025		SER	



(b) (6), (b) (7)(E)

Sun (Software)	Sun (Hardware)	Solaris		Password - Compromised	7028	SER
Sun (Software)	Sun (Hardware)	Solaris 2.5		Undetermined	7033	SER
Sun (Software)	Sun (Hardware)	Solaris		Undetermined	7035	SER
Sun (Software)	Sun (Hardware)	Solaris		Password - Compromised	7042	SER
DEC	DEC	Other (Software)		Password - Compromised	7024	SER
Sun (Software)	Sun (Hardware)	Solaris		Password - Compromised	7026	SER
Sun (Software)	Sun (Hardware)	Solaris		Password - Compromised	7027	SER
Sun (Software)	Sun (Hardware)	Solaris		Password - Compromised	7029	SER
Sun (Software)	Sun (Hardware)	Solaris		SolSadmindAmslverifyBo	7030	SER
Sun	Sun	Solaris		Passw	7031	PU

(b) (6), (b) (7)(E)	Sun (Software)	Sun (Hardware)	Solaris	Password - Compromised	7032	PUB
	Sun (Software)	Sun (Hardware)	Solaris	Undetermined	7034	SER
	Sun (Software)	Sun (Hardware)	Solaris	SolSadmindAmslverifyBo	7039	SER
	Sun (Software)	Sun (Hardware)	Solaris	SolSadmindAmslverifyBo	7041	PUB
	Sun (Software)	Sun (Hardware)	Solaris	Password - Compromised	7040	SER
	Sun (Software)	Sun (Hardware)	Solaris	Undetermined	7036	SER
	Sun (Software)	Sun (Hardware)	Solaris	SolSadmindAmslverifyBo	7037	SER

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41555

Additional Information

Notices

ID	Abbreviation	noticeid	Date
No Records Found			



Summary: All of the affected hosts were partitioned from the network and then rebuilt from source media. All passwords of all hosts on the affected network segments were changed. All telnet and ssh access was temporarily suspended and considerable justification is being required, along with verification of the security posture of the system, before access is reinstated. 04/12/2004:

Chronology: On January 25th a valid Langley user account was accessed from a system at CalTec via ssh. The owner of the account is located at the University of Colorado. It has been determined that she used the same password on numerous systems. The intruder then began scanning the Langley network for systems with samba, ftp and sadmind vulnerabilities over the next 2 days until telnet and ssh access was blocked. By exploiting these vulnerabilities (primarily sadmind and samba) and through some existing trust relationships between systems, he eventually gained access to 22 systems. It has been determined that he gained root access on all but one of the 22 systems. As he gained access to a system, he frequently ftp?d to ftp.uu.net to download malware. He installed rootkits, including sniffers, on several of the systems. On January 25th a valid Langley user account was accessed from a system at CalTec via ssh. The owner of the account is located at the University of Colorado. It has been determined that she used the same password on numerous systems. The intruder then began scanning the Langley network for systems with samba, ftp and sadmind vulnerabilities. By exploiting these vulnerabilities (primarily sadmind and samba) and through some existing trust relationships between systems, he eventually gained access to 22 systems. It has been determined that he gained root access on all but one of the 22 systems. As he gained access to a system, he frequently ftp?d to ftp.uu.net to download malware. He installed rootkits, including sniffers, on several of the systems. ** -----Original Message----- From: b6, 7C [mailto:b6, 7C asa.gov] b6, 7C April 12, 2004 4:13 PM To: (b) (6), (b) (7)(C) nasa.gov; nasirc@nasirc.hq.nasa.gov Cc: b6, 7C nasa.gov Subject: (NASIRC Ref: 107412725) F NASA Machines At first glance, this does appear to be the January incident b6, X-Sender: b6, 7C gov >X-Mailer: QUALCOMM Windows Eudora Version 5.2.1 >Date: Mon, 12 Apr 2004 13:0 b6, 7C nasa.gov >From: b b6, >Subject: CIAC CASE 596 NASA Machines >Cc: ciac@ciac.org > >b6, 7C , > >Below is the list of compromised machines at NASA. Please pass the JPL >list to your counterpart there. This list was obtained from an e-mail from >the intruder where he was bragging that he owned these machines. He has >ben targeting UNIX boxes, including Linux, Solaris, and AIX. > >On the Linux boxes he uses a variant of the SK rootkit. I have attached a >detector containing his current SK password. The detector uses his client >application to see if the back door will open with this password. If it >does, you know you are compromised. The hidden file suffix for this >rootkit is xrk. Any file that ends with those letters is hidden so a quick >local test is to use touch to create a file that ends with those letters >and see if it is hidden. For example, > >touch myxrk >ls > >If myxrk does not appear in the listing, you are compromised. >Rootkit info >Hidden file suffix: xrk >Home directory: /etc/k.xrk >Hidden copy of init /sbin/initxrk >Detector: ciaclogin11 > >Note that this detector will work until the intruder changes the password, >but that does not happen often because the password is compiled into the >rootkit. > >The script included with the detector scans the detector over a subnet and >interprets the results. > >For other unix systems, the intruder is using Trojaned versions of >OpenSSH, in.ftpd, and ftp. All of these Trojans collect usernames and >passwords and send them to (b) (6), (b) (7)(C) and to port 55 on >fooshfoosh.ath.cx which currently points to mcc.atmos.colostate.edu >(129.82.48.87) (I mixed up the machines when I talked to you on the >phone). Note that fooshfoosh is a dynamic DNS name and the address it >points to has changed a few times. If you nave netflow data showing port >55 connections to whatever address fooshfoosh is pointing to, those >machines are probably compromised. > >Let me know if you have any questions. > b6, 7C /CIAC > >NASA - LARC b6, 7C arc.nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >128.155.10.187 nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov > >NASA - JPL >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) nasa.gov >(b) (6), (b) (7)(E) .nasa.gov >(b) (6), (b) (7)(E) nasa.gov > > >-- b6, 7C b6, 7C gov b6, 7C >PGP Fingerprint: 93D1 5A0A EC46 665D 47A4 42FC A74C 6CB4 >Computer Incident Advisory Capability - CIAC > Lawrence Livermore National Lab > P.O. Box 808, L-303 > Livermore, CA 94551 > CIAC Phone: b6, 7C , Fax: (b) (6), (b) (7)(C) > E-mail: ciac@ciac.org virus samples to: virusin@ciac.org >-- b6, 7C ,CISSP b6, 7C @nasa.gov NASA Langley Research Center Information Technology Security Manager PH: b6, 7C FAX: (b) (6), (b) (7)(C) Cell: b6, b6, 7C

ask about these highlights

NASIRC Notes:



200141262

General Information

Record Number:	200141262	**Center:**	GSFC
Title:	Password file		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	GSFC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	13600
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C) nasa.gov
		Source of Report:	Lead System Administrator
		Est. Cost (hours):	136

Incident Dates

Incident Date:	3/18/2004	**Incident Zone:**	GMT
Discovered Date:	3/18/2004	**Discovered Zone:**	EST
NASIRC Notified Date:	3/22/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	4/14/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	3/18/2004	**ITSM Zone:**	EST
US-CERT Date:		**US-CERT Zone:**	
CSO Date:	3/18/2004	**CSO Zone:**	EST
OIG Date:	3/18/2004	**OIG Zone:**	GMT
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)		(b) (6), (b) (7)(C)	SGI	Unknown	IRIX 6.5		Workstation					900.3	Password - Compromised	7228		SER	
			SGI	Unknown	IRIX	Unknown	Workstation					900.3	Password - Compromised	7229		SER	
			SGI	Unknown	IRIX	Unknown	Workstation					900.3	Password - Compromised	7230		SER	
			SGI (Software)		IRIX		Server : Mail					912	Account - User	8181		ADM	
			Debian	Intel	Other		Server : Workgroup					931	Account - User	8182		ADM	
			SGI (Software)		IRIX 6.5		Server :					900.3	Account -	8183		ADM	

SENSITIVE BUT UNCLASSIFIED

(b) (6), (b) (7)(E)

re)			Workg roup		User		
			Unkno wn	931	Accou nt - User	8184	SER
GI Softw re)		IRIX	Works tation	916	Accou nt - User	8185	SER
		Linux	Works tation	931	Accou nt - Guest	8186	SER
		Linux 6.2	Works tation	680	Accou nt - User	8187	SER
un Softw re)	Sun (Hard ware)	Solaris	Sparc 10	931	Accou nt - User	8188	SER
		Linux	Works tation	931	Accou nt - User	8189	SER
un Softw re)		Solaris		931	Accou nt - User	8190	SER
GI Softw re)		IRIX	Works tation	916	Accou nt - User	8191	SER
GI Softw re)		IRIX		931	Accou nt - User	8192	SER
GI Softw re)		IRIX		931	Accou nt - User	8193	SER
edha		Linux 6.2	Works tation	661	Accou nt - Guest	8194	SER
edha		Linux 6.2		931	Accou nt - User	8195	SER

(b) (6), (b) (7)(E)

	SGI (Software)		IRIX		931	Account - User	8196	SER
	Other (Software)		Other	Workstation	921	Account - User	8197	SER
	SGI (Software)		IRIX	Workstation	931	Account - User	8198	SER
	SGI Software)		IRIX		931	Account - User	8199	SER
	Sun (Software)	Sun (Hardware)	SolarisSun		560		8200	SER
					931	Local Root Exploit	8201	SER
				Server : Workgroup	926	Account - User	8202	SER
				Workstation	912	Linux ptrace() kmod	8203	SER
	SGI (Software)		IRIX	Server : Workgroup	975		8204	SER
							8205	
	SGI (Software		IRIX		680	Account -	8207	SER



(b) (6), (b) (7)(E)	(b) (6), (b) (7)(C)	SGI (Software)	IRIX	680	Account - User	8208	SER
		SGI (Software)	IRIX	680	Account - User	8209	SER
		SGI (Software)	IRIX	680	Account - User	8210	SER

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41570
	41571
	41572

Additional Information

Notices

ID	Abbreviation	noticeid	Date
No Records Found			

Summary:	3/22/2004: At present these systems are blocked. The (b) (6), (b) (7)(C) (OIG s) is comfortable with log files and backups that were provided to b6, by the Code 297 IRT. Zeus, tropic and luz will be unblocked today. The lead system administrator will change the password on the affected user s account and review the .shost & .rhost files.
Chronology:	3/22/2004: On 2004-03-18, a lead systems administrator reported three GSFC systems had account compromises deriving from a UCAR host on 2004-03-16. The user whose account had been compromised reported that the same account password was present on the UCAR host and the first of the three GSFC hosts. The remaining two GSFC hosts are believed to have been compromised via the use of .rhosts or .shosts. The initial extent of the compromise was greatly aided by the fact that the local organization employs a centralized logging host.
NASIRC Notes:	



SENSITIVE BUT UNCLASSIFIED

200141270

General Information

Record Number:	200141270	**Center:**	GSFC
Title:	Information Compromise		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	GSFC	**Coordinator:**	b6, 7C
Incident Category:	Information Compromise	**Est. Cost ($):**	4300
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C
		Source of Report:	DCSE
		Est. Cost (hours):	43

Incident Dates

Incident Date:	3/24/2004	**Incident Zone:**	EST
Discovered Date:	3/24/2004	**Discovered Zone:**	EST
NASIRC Notified Date:	3/25/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	6/18/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	3/24/2004	**ITSM Zone:**	EST
US-CERT Date:		**US-CERT Zone:**	
CSO Date:	3/24/2004	**CSO Zone:**	EST
OIG Date:	3/24/2004	**OIG Zone:**	EST
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

ask if the highlighted texts are names of individuals?

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Redhat		Linux 7.x							916	Linux ptrace() kmod	7255		SER	
			Redhat		Linux 7.x							916	Linux ptrace() kmod	7256		SER	
			Redhat		Linux 7.x							916	Linux ptrace() kmod	7257		SER	

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41577
	41578
	41579
	41580
	41581

Additional Information



Notices

ID	Abbreviation	noticeid	Date

No Records Found

Summary:	3/25/2004: These systems are blocked and are being investigated... 6/18/2004: Two of the three systems will be rebuilt and scanned in order to return to the service; the other system will be excessed.
Chronology:	3/25/2004: On 2004-03-24, Code 916 reported suspicious scanning originating from a GSFC host. Upon investigation by the responsible system administrator,with the aide of a central logging host, three user level compromises were discovered. The compromises derived from recent NOAA system-level compromises. Code 297 IDS logs confirm several SSH sessions and a local sendmail exploit download around this time. The system administrator for the compromised hosts, b6, 7C , contacted the user "b6, " about SSH logins from several NOAA systems in the 04:00 EST hour. The user confirmed that those sessions were not legitimate. At that time, the user informed b6, 7C of the NOAA compromises. b6, 7C has been in contact with the NOAA CIRT, who provided details about their compromises. The NOAA CIRT reported to b6, 7C that a Linux ptrace exploit was responsible for their system-level compromises. b6, 7C also stated that the systems are not running Sendmail. At this time, no other exploit downloads have been detected. The local exploits were retrieved from a packetstorm. org mirror site, so it will not be considered a hostile. A number of other systems were seen conducting SSH traffic with the compromised hosts, but those have been identified as normal activity by b6, 7C NOAA CIRT identifed several additional hosts that were compromised in their network:
NASIRC Notes:	



200141278

General Information

Record Number:	200141278	**Center:**	GSFC
Title:	Unauthorized Access		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	GSFC	**Coordinator:**	b6, 7C
Incident Category:	Unauthorized Access	**Est. Cost ($):**	
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C gsfc.nasa.gov
		Source of Report:	MSFC IT Security Team
		Est. Cost (hours):	

Incident Dates

Incident Date:	4/7/2004	**Incident Zone:**	GMT
Discovered Date:	4/7/2004	**Discovered Zone:**	CST
NASIRC Notified Date:	4/8/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	6/7/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	4/17/2004	**ITSM Zone:**	EST
US-CERT Date:		**US-CERT Zone:**	
CSO Date:	4/8/2004	**CSO Zone:**	EST
OIG Date:	4/8/2004	**OIG Zone:**	EST
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)		b6, 7C	(Software)		Solaris 9		Research/Testing					295	Undetermined	7271		BRT	

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41598
(b) (6), (b) (7)(E)	41599
(b) (6), (b) (7)(E)	41600

Additional Information

Notices

ID	Abbreviation	noticeid	Date
No Records Found			

Summary: 4/8/2004: The Deputy, ITSM was notified by NISN IT Security on 4/7/2004, at approximately 1915 hrs on compromised host telenet actiity with a Romanian host. The hostile site was blocked by NISN. At approximately 2000 hrs the Deputy, ITSM was contacted by NISN IT Security and was conference called in with b6, 7C and b6, b6, , the Deputy, ITSM asked b6, to block the compromised host both inbound/outbound until 4/8/2004. The compromised host is now off-line and blocked at the firewall. In addition the hostiles are blocked as well. The CI Officer and OIG have been notified of the incident. 6/7/2004: Incident hours will be updated.

Chronology:	4/8/2004: Executive Summary ================= On 2004-04-07 Code 297 IDS detected unusual the execution of commands indicitive of a compromise inside of a telnet session involving a GSFC system and a Romanian hostile. Further examination of examined network traces showed the system was compromised, and most likely some time prior to 2004-04-07. At this time the actual method of comprimise is unknown. NISN reported unusual telnet activity involving the same GSFC system including "SYN, FIN, PUSH, and RST packets". While it is unusual to see packets with the PUSH flag set, the observed behavior was unrelated to the actual compromise of the system. Summary ======= Network trace data from 2004-04-07 at approximately 22:16 GMT shows the hostile party logging into the GSFC system using the account "bellea", and then changing users to "rewt". The presence of the "rewt" account indicates the system was compromised prior to the observed telnet traffic. The hostile party then proceeded to download a Solaris root kit(the installation failed) and installed the PsyBNC IRC proxy. Data transmitted during the session indicates a previous login from b6, 7C .
NASIRC Notes:	



200141281

General Information

Record Number:	200141281	**Center:**	GSFC
Title:	System Compromise		
Contact Name:	b6, 7C	**Contact Phone:**	
Contact Center:	GSFC	**Coordinator:**	b6, 7C
Incident Category:	System Compromise	**Est. Cost ($):**	4200
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	b6, 7C .nasa.gov
		Source of Report:	NISN
		Est. Cost (hours):	42

Incident Dates

Incident Date:	4/12/2004	**Incident Zone:**	GMT
Discovered Date:	4/12/2004	**Discovered Zone:**	GMT
NASIRC Notified Date:	4/13/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	4/16/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	4/12/2004	**ITSM Zone:**	GMT
US-CERT Date:		**US-CERT Zone:**	
CSO Date:	4/12/2004	**CSO Zone:**	GMT
OIG Date:	4/12/2004	**OIG Zone:**	GMT
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information

PII Involved?:	No	PII Report Date:	
PII Disclosed By:		PII Data Protection:	Unknown
PII Data Types:			
Scope of PII Exposure:		Number of Unauthorized People with Access:	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E), (b) (7)(C)		b6, 7C	IBM		AIX		Workstation				4242,25841		Not listed - Described in Comments	7274		SER	
		b6, 7C	IBM		AIX		Server : Application				4242,25841		Not listed - Described in Comments	7275		SER	

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41601
(b) (6), (b) (7)(E)	41602

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-100	NASIRC	3301	14-APR-2004

Summary: 4/13/2004: Both systems and hostiles are blocked at the firewall. These systems will be rebuilt and scan before they are authorized back into the CNE evnironment. 6/4/2004: IRT (10) Incident hours updated.. 7/24/2004: Incident hours updated by affecting organization 24 hrs previously reported final report indicates 32.

Chronology: 4/13/2004: A report from NISN regarding hostile probing was reported on 2004-04-12. Initial investigation reveals that on 2004-04-12 starting at 16:56:43 GMT, hostile attacks against port 4242/tcp were detected. At 17:00:21 and 17:02:27 GMT on the same day, two AIX machines sustained system compromises. Another attack was seen against port 21/tcp on a couple of host, but those were unsuccessful. The intruder appears to have had some difficulty compiling source code on one of the machines and trouble FTPing files on the other. Both systems were exploited via Service on port 4242/tcp

NASIRC Notes:



200141287

General Information

Record Number:	200141287	**Center:**	JPL
Title:	(b) (6), (b) (7)(E) jpl.nasa.gov ((b) (6), (b) (7)(E)) Compromised		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	
Incident Category:	Unauthorized Access	**Est. Cost ($):**	1100
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C) nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	11

Incident Dates

Incident Date:	4/14/2004	**Incident Zone:**	PDT
Discovered Date:	4/21/2004	**Discovered Zone:**	
NASIRC Notified Date:	4/23/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	5/26/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Linux		Linux			ITAR	486				Account - User	7398	Y	N/A	

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41912

Additional Information

Notices

ID	Abbreviation	noticeid	Date
(b) (6), (b) (7)(E)-ID130-04-	Center	3296	26-APR-2004

Summary: 05/07/2004: 3 additional JPL systems were added per weekly incident report from (b) (6), (b) (7)(C) at JPL (b) (6), (b) (

SENSITIVE BUT UNCLASSIFIED

Chronology:	-----Original Message----- From: (b) (6), (b) (7)(C) nasa.gov [mailto:(b) (6), (b) (7)(C) nasa.gov] Sent: Friday, April 23, 2004 9:55 AM To: (b) (6), (b) (7)(E) hq.nasa.gov; (b) (6), (b) (7)(C) nmo.jpl.nasa.gov; (b) (6), (b) (7)(C) asa.gov; (b) (6), (b) (7)(C) jpl.nasa.gov; (b) (6), (b) (7)(E) hq.nasa.gov; security@telchar.jpl.nas (NASIRC Ref: 107414347) JPL Incident Initial Notification (ID_130) INITIAL INCIDENT NOTIFICATION Investigation Name:(b) (6), (b) (7)(E) -ID130-04-2004 Incident Date:2004-04-14, 14:04 Investigator Name:(b) (6), (b) (7)(C) Notified By:External Site JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Linux Kernel | n/a | UA | User Account | Yes | ITAR Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Bethlehem | PA | United States Sensitive Information Involved:Yes Description of Sensitive Information Involved:ITAR Additional Information:None. NASIRC Action:None. -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C) .jpl.nasa.gov] Sent: Monday, April 26, 2004 6:10 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) asa.gov Subject: (NASIRC Ref: 107414794) Weekly Incident Report for 16Apr04_25 ********************************* NEW INCIDENTS: 1 ** INCIDENT INFO Incident Name:(b) (6), (b) (7)(E) -ID130-04-2004 Discovery Date:21-APR-04 Exploit Date:14-APR-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Linux Kernel OS Version:n/a System Security Plan:486 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 9 OS Version:n/a System Security Plan:n/a -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C) jpl.nasa.gov] Sent: Friday, May 07, 2004 5:46 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov Subject: (NASIRC Ref: 107417505) Weekly Incident Report for 30Apr04_06May04 INCIDENT INFO Incident Name:ICE--ID131-04-2004 Discovery Date:27-APR-04 Exploit Date:22-APR-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) Hostile Name:(b) (6), (b) (7)(E) Hostile IP(b) (6), (b) (7)(E) Hostile Name(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E) jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:SSL_PCT1_Overflow System OS:MS Windows 2000 OS Version:2K System Security Plan:304 Domain Name:(b) (6), (b) (7)(E) jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:SSL_PCT1_Overflow System OS:MS Windows 2000 OS Version:2k System Security Plan:n/a Domain Name(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:SSL_PCT1_Overflow System OS:MS Windows 2000 OS Version:2k System Security Plan:273 Domain Name:(b) (6), (b) (7) jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:SSL_PCT1_Overflow System OS:MS Windows 2000 OS Version:2k System Security Plan:383 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:SSL_PCT1_Overflow System OS:MS Windows 2000 OS Version:2K System Security Plan:85 Domain Name:(b) (6), (b) (7)(E) jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:SSL_PCT1_Overflow System OS:MS Windows 2000 OS Version:2k System Security Plan:442 Domain Name:(b) (6), (b) (7)(E) jpl.nasa.gov IP Address(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:SSL_PCT1_Overflow System OS:MS Windows 2000 OS Version:2K System Security Plan:304
NASIRC Notes:	



200141289

General Information

Record Number:	200141289	**Center:**	JPL
Title:	(b) (6), (b) (7)(E) ((b) (6), (b) (7)(E)) Compromised		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Non-Incident	**Est. Cost ($):**	1100
Attacker:	Stakkato/stkto	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C) nasirc.nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	11

Incident Dates

Incident Date:	4/14/2004	**Incident Zone:**	
Discovered Date:	4/21/2004	**Discovered Zone:**	
NASIRC Notified Date:	4/26/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	5/27/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



SENSITIVE BUT UNCLASSIFIED

PII Involved?:	No	PII Report Date:	
PII Disclosed By:		PII Data Protection:	Unknown
PII Data Types:			
Scope of PII Exposure:		Number of Unauthorized People with Access:	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Software)		Solaris 9									7400			

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41913

Additional Information

Notices

ID	Abbreviation	noticeid	Date
ARCTICWOLF-ID130-04-	Center	3295	26-APR-2004

Summary: 05/27/2004: Corbin indicated that this is a False/Positive and part of Articwolf case (200141287).

Chronology: -----Original Message----- From: (b) (6), (b) (7)(C) [(b) (6), (b) (7)(C) jpl.nasa.gov] Sent: Monday, April 26, 2004 6:10 PM To: nasirc@nasirc.hq.nasa.gov (b) (6), (b) (7)(C) sa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov Subject: (NASIRC Ref: 107414794) Weekly Incident Report for 16Apr04_25Apr04 ** NEW INCIDENTS: 1 ** INCIDENT INFO Incident Name:(b) (6), (b) (7)(E)-ID130-04-2004 Discovery Date:21-APR-04 Exploit Date:14-APR-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Linux Kernel OS Version:n/a System Security Plan:486 Domain Name:(b) (6), (b) (7)(E) jpl.nasa.gov IP Address:137.79.125.117 Incident Category:System Compromise Exploit Used:Undetermined System OS:Sun Solaris 9 OS Version:n/a System Security Plan:n/a

NASIRC Notes:	



200141290

General Information

Record Number:	200141290	**Center:**	ARC
Title:	NAS compromise(Now part of Incident 200141309)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	ARC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	
Attacker:	Stakkato/stkto	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	Unknown
		Contact Email:	(b) (6), (b) (7)(C)@nasa.gov
		Source of Report:	
		Est. Cost (hours):	

Incident Dates

Incident Date:	4/22/2004	**Incident Zone:**	
Discovered Date:	4/22/2004	**Discovered Zone:**	
NASIRC Notified Date:	4/26/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	6/3/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
	0.0.0.0		Unknown		Other								Undetermined	7756		N/A	

Hostile Site Information

IP Address	hostile_site_id
0.0.0.0	41920

Additional Information

Notices

ID	Abbreviation	noticeid	Date
No Records Found			

Summary:	This incident is now part of Incident 200141309.
Chronology:	On Thursday April 22, 2004 at approx. 4pm IT Security was notified by the security group at the NAS facility that they had encountered an incident with one of their supercomputers where they found a user level compromise. The OIG and ITSM were notified immediately. An agreement between the OIG, NAS and ITSM stated that the system would remain online unless evidence of a root level compromise occured. The system is currently being reviewed by the security team at the NAS facility
NASIRC Notes:	This incident is possibly related to incidents at JPL and GSFC.



SENSITIVE BUT UNCLASSIFIED

200141299

General Information

Record Number:	200141299	**Center:**	JPL
Title:	System Compromises at JPL (JPL ID 132)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	20000
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C) nasirc.nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	200

Incident Dates

Incident Date:	4/17/2004	**Incident Zone:**	PDT
Discovered Date:	5/4/2004	**Discovered Zone:**	
NASIRC Notified Date:	5/5/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	3/7/2005	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	300

PII Information

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Redhat		Linux 7.x				506				Undetermined	7649		SER	CAT 1



							System Compromise
(b) (6), (b) (7)(E)	Sun (Software)	Solaris 8	132	Password - Compromised	7705	SER	CAT 1 Un-

							System Compromise
(b) (6), (b) (7)(E)	Sun (Software)	Solaris 2.6	132	Password - Compromised	7706	SER	CAT 1 Un-



							System Compromise
(b) (6), (b) (7)(E)	Redhat	Linux 7.x	506	Password - Compromised	7711	SER	CAT 1 Una



							System Compromise
(b) (6), (b) (7)(E)	Sun (Software)	Solaris 2.6	274	Local Root Exploit	7752	SER	CAT 1 U

							System Compromise
(b) (6), (b) (7)(E)	Linux	Linux	506	Local Root Exploit	7753	SER	CAT 1 U

							System Compromise
(b) (6), (b) (7)(E)	Sun (Software)	Solaris 2.5	93	Local Root Exploit	7834	SER	CAT 1



						Sys te m Co mp ro mis e
(b) (6), (b) (7)(E)	Linux	Linux	Local Root Exploit	7835	SER	CAT 1 U n

						System Compromise
(b) (6), (b) (7)(E)	Sun (Software)	Solaris 9	Local Root Exploit	7836	SER	CAT 1 U

							System Compromise
(b) (6), (b) (7)(E)	Sun (Software)	Solaris 8	503	Local Root Exploit	7768	SER	CAT 1



SENSITIVE BUT UNCLASSIFIED

							System Compromise
(b) (6), (b) (7)(E)	SuSE	Linux 8.0	73	Local Root Exploit	7770	SER	CAT 1 U



							System Compromise
(b) (6), (b) (7)(E)	Redhat	Linux	372	Linux ptrace() kmod	7771	SER	CAT 1

							System Compromise
(b) (6), (b) (7)(E)	Redhat	Linux 7.x	132	Local Root Exploit	7772	SER	CAT 1

						System Compromise
(b) (6), (b) (7)(E)	Redhat	Linux	Local Root Exploit	7773	SER	CAT 1

						System Compromise
(b) (6), (b) (7)(E)	Redhat	Linux 7.x	Linux ptrace() kmod	7774	SER	CAT 1



							System Compromise
(b) (6), (b) (7)(E)	Sun (Software)	SolarisSun 2.6	245	Local Root Exploit	7775	SER	CAT 1



							System Compromise
(b) (6), (b) (7)(E)	SGI	IRIX 6.5	144	Local Root Exploit	7776	SER	CAT 1



Sys
te
m
Co
mp
ro
mis
e

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41946
	41947
	41948
	41949
	41950
	41943
	41944
	41945
	41924
	41925



(b) (6), (b) (7)(E)	
	41914
	41921
	41922
	41923
	41959

Additional Information

Notices

ID	Abbreviation	noticeid	Date
107491869	Mail Handler	3575	14-MAR-2005
A-04-126	NASIRC	3305	05-MAY-2004
A-04-126-A	NASIRC	3361	07-MAY-2004
A-04-126-B	NASIRC	3362	01-JUN-2004
A-04-126-C	NASIRC	3363	08-JUN-2004
A-04-126-D	NASIRC	3364	21-JUN-2004
A-04-126-E	Mail Handler	3365	22-JUN-2004
A-04-126-F	NASIRC	3366	28-JUN-2004
A-04-126-G	NASIRC	3367	19-JUL-2004
JPL ID 132	Center	3438	09-SEP-2004
VXSERVER-ID132-05-20	Center	3300	05-MAY-2004

Summary: 05/05/2004: NASIRC received a report from (b) (6), (b) (7)(C) @ JPL with information regarding the compromise of NASA system 137.78.65.82. NASIRC issued an alert. (LS) 05/07/2004: Updated incident PER (b) (6), (b) (7)(C) Weekly Incident Report 5 additional JPL systems compromise, 2 unauthorized access, 1 undetermined category. Listed below Talked to (b) (6), (b) (7)(C) about issuing a followup alert. He said ok ((b) (6), (b 05/10/2004: Seperated the System Compromises, Unauthorized Accessed Systems and Undetermined Category into three seperate incidents. ((b) (6), (b 200141304, Unauthorized Access Incident 200441305, Other IT Concern Incident 200141299, System Compromise Incident 06/25/2004: More updates added per weekly incident report. ((b) (6), (b

SENSITIVE BUT UNCLASSIFIED

Chronology:	-----Original Message----- From: (b) (6), (b) (7)(C) nasa.gov [mailto (b) (6), (b) (7)(C) nasa.gov] Sent: Wednesday, May 05, 2004 11:49 AM To: jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) jpl.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) .jpl.nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa NASIRC Ref: 107416469) JPL Incident Initial Notification (ID_ (b) (6),) INITIAL INCIDENT NOTIFICATION Investigation Name: (b) (6), (b) (7)(E) (b) (6), (b) (7)(E) Incident Date:2004-04-17, 07:07 Investigator Name: (b) (6), (b) (7)(C) Notified By:NASIRC JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 7.x | n/a | SC | Undetermined | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | n/a | PA | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. -----Original Message----- From: (b) (6), (b) (7)(C) [mailto: (b) (6), (b) (7)(C) jpl.nasa.gov] Sent: Friday, May 07, 2004 5:46 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov Subject: (NASIRC Ref: 107417505) Weekly Incident Report for 30Apr04_06 *********************************** NEW INCIDENTS: 1 ** INCIDENT INFO Incident Name:VXSERVER-ID (b) (6), (b) (7)(E) Discovery Date:04-MAY-04 Exploit Date:17-APR-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name: (b) (6), (b) (7)(E) Hostile IP: (b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name (b) (6), (b) (7)(E) .jpl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a Domain Name: (b) (6), (b) (7)(E) pl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:132 Domain Name: (b) (6), (b) (7)(E) jpl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:132 Domain Name: (b) (6), (b) (7)(E) .jpl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:506 Domain Name (b) (6), (b) (7)(E) .jpl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:131 Domain Name (b) (6), (b) (7)(E) .jpl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:MKLinux OS Version:n/a System Security Plan:506 Domain Name: (b) (6), (b) jpl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:Unknown Exploit Used:Undetermined System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a Domain Name: (b) (6), (b) (7)(E) .jpl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:506 Domain Name: (b) (6), (b) (7)(E) .jpl.nasa.gov IP Address: (b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:506
NASIRC Notes:	06/09/2004: -----Original Message----- From: (b) (6), (b) (7)(C) [mailto: (b) (6), (b) (7)(C) nasa.gov] Sent: Tuesday, June 08, 2004 2:53 PM To: (b) (6), (b) (7)(C) ; nasirc@nasirc.hq.nasa.gov Cc: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) Subject: (NASIRC Ref: 107428520) Re: JPL incident will go beyond 30 day mark Extension approved. M *** 6/7/04: JPL requested extension to close. -----Original Message----- From: (b) (6), (b) (7)(C) [mailto: (b) (6), (b) (7)(C) asa.gov] Sent: Monday, June 07, 2004 11:23 AM To: nasirc@nasirc.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov Cc: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) Subject: (NASIRC Ref: 107428173) JPL incident will go beyond 30 day mark Upon reviewing the open JPL incidents, I see that incident # 200141299 has gone beyond it s 30 mark of Jun 6th. We have added 2 new compromised hosts to this incident and may not be able to complete the investigation and incident summary by the deadline. (b) (6), (b) (7)(C) P.S. Had to remove (b) (6), (b) (7)(C) as Ames PKI seems to be unavailable - I ll forward this to him as soon as I can. -- (b) (6), (b) (7)(C) JPL IT Security Operations Lead ETS Service Engineer JPL SAGE Chair ICIS Office, Jet Propulsion Laboratory Public PGP key: (b) (6), (b) (7)(C), (b) (7)(E) 07/19/2004: NASIRC received the weekly incident update. NASIRC up dated this incident. ((b) (6))



200141304

General Information

Record Number:	200141304	**Center:**	JPL
Title:	Unauthorized Access of Six JPL Systems (JPL ID 132)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	4800
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C) nasirc.nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	48

Incident Dates

Incident Date:	4/17/2004	**Incident Zone:**	
Discovered Date:	5/4/2004	**Discovered Zone:**	
NASIRC Notified Date:	5/10/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	3/7/2005	**Closed Zone:**	EST

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	300

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Redhat		Linux								Account - User	7720		SER	CAT 1 U

							User Compromise
(b) (6), (b) (7)(E)	Redhat	Linux	131	Account - User	7721	SER	CAT 1 Un-



						User Compromise
(b) (6), (b) (7)(E)	Sun (Software)	Solaris 8	Account - User	7754	SER	CAT 1 U

						User Compromise
(b) (6), (b) (7)(E)	Sun (Software)	Solaris 8	Account - User	7837	SER	CAT 1 U

							User Compromise
(b) (6), (b) (7)(E)	SGI	SGI	IRIX 6.5	SSL_PCT1_Overflow	7777	SER	CAT 1

								User Compromise
(b) (6), (b) (7)(E)	SGI	SGI	IRIX 6.5	Unknown	Account - User	7781	SER	CAT 1 U

User Compromise

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41936
	41937
	41938
	41939
	41940
	41941
	41942
	41926
	41927
	41928
	41929



(b) (6), (b) (7)(E)	
	41930
	41935
	41618
	41960

Additional Information

Notices

ID	Abbreviation	noticeid	Date
107491869	Mail Handler	3576	14-MAR-2005
A-04-126	NASIRC	3368	05-MAY-2004
A-04-126-A	NASIRC	3369	07-MAY-2004
A-04-126-B	NASIRC	3370	01-JUN-2004
A-04-126-C	NASIRC	3371	08-JUN-2004
A-04-126-D	NASIRC	3372	21-JUN-2004
A-04-126-E	NASIRC	3373	22-JUN-2004
A-04-126-F	NASIRC	3374	28-JUN-2004
A-04-126-G	NASIRC	3375	19-JUL-2004
JPL ID 132	Center	3439	09-SEP-2004
VXSERVER-ID132-05-20	Center	3306	25-JUN-2004

Summary: 05/10/2004: Seperated the System Compromises, Unauthorized Accessed Systems and Undetermined Category into three seperate incidents. (b) (6), (b) 200141304, Unauthorized Access Incident 200441305, Other IT Concern Incident 200141299, System Compromise Incident

Chronology: -----Original Message----- From: (b) (6), (b) (7)(C) [mailto (b) (6), (b) (7)(C) enigma.jpl.nasa.gov] Sent: Friday, May 07, 2004 5:46 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov Subject: (NASIRC Ref: 107417505) 0Apr04_06May04 ** NEW INCIDENTS: 1 ** INCIDENT INFO Incident Name:VXSERVER-ID132-05-2004 Discovery Date:04-MAY-04 Exploit Date:17-APR-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E) jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:132 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:132 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:506 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:1(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:131 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:MKLinux OS Version:n/a System Security Plan:506 Domain Name:(b) (6), (b) .jpl.nasa.gov IP Address:1(b) (6), (b) (7)(E) Incident Category:Unknown Exploit Used:Undetermined System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:506 Domain Name:(b) (6), (b) (7)(E) .jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:506

NASIRC Notes:	06/09/2004 -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C) nasa.gov] Sent: Tuesday, June 08, 2004 2:53 PM To: (b) (6), (b) (7)(C) nasirc@nasirc.hq.nasa.gov Cc: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) Subject: (NASIRC Ref: 107428520) Re: JPL incident will go beyond 30 day mark Extension approved. M 07/19/2004: NASIRC received the JPL weekly incident update. NASIRC up dated this incident. (LS)



200141305

General Information

Record Number:	200141305	**Center:**	JPL
Title:	(b) (6), (b) (7)(E) jpl.nasa.gov Category Non-Incident		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Non-Incident	**Est. Cost ($):**	100
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C) nasirc.nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	1

Incident Dates

Incident Date:	4/17/2004	**Incident Zone:**	
Discovered Date:	5/4/2004	**Discovered Zone:**	
NASIRC Notified Date:	5/10/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	6/8/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Redhat		Linux								Undetermined	7719			
			Linux						506					7778			
			Linux						506					7779			

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41915

Additional Information

Notices

ID	Abbreviation	noticeid	Date
(b) (6), (b) (7)(E)	Center	3303	01-JUN-2004

Summary:	06/21/04: Added (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E) to this incident issued follow-up to change category to non-incident, ok d with (b) (6), (b) (7)(C) 06/08/2004: (b) (6), (b) was a false positive. User had legit accounts on NAS and all were accounted for. (b) (6), (b) (7)(C) 05/10/2004: Entered this incident as an Other IT Concern because the category was Undetermined. (b) (6), (b) 05/10/2004: Seperated the System Compromises, Unauthorized Accessed Systems and Undetermined Category into three seperate incidents. (b) (6), (b) 200141304, Unauthorized Access Incident 200441305, Other IT Concern Incident 200141299, System Compromise Incident
Chronology:	-----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C)jpl.nasa.gov] Sent: Friday, May 07, 2004 5:46 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov Subject: (NASIRC Ref: 107417505) Weekly Incident Report for 30Apr04_06May04 ** NEW INCIDENTS: 1 ** INCIDENT INFO Incident Name:(b) (6), (b) (7)(E)-ID(b) (6), (b) (7)(E) Discovery Date:04-MAY-04 Exploit Date:17-APR-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E)pl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:132 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:132 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:506 Domain Name(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:131 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E)Incident Category:System Compromise Exploit Used:Root account cracked System OS:MKLinux OS Version:n/a System Security Plan:506 Domain Name:(b) (6), (b).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unknown Exploit Used:Undetermined System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a Domain Name(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:506 Domain Name:(b) (6), (b) (7)(E).jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Undetermined System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:506 06/08/2004: (b) (6), (b) was a false positive. User had legit accounts on NAS and all were accounted for. (Corbin)
NASIRC Notes:	6/8/04: JPL changed category for (b) (6), (b) to non-incident. 6/18/04: JPL reported(b) (6), (b) (7)(E) and (b) (6), (b) (7)(E) as False alarm. 6/22/04: Per (b) (6), (b) (7)(C) add (b) (6), (b) (7)(E) AND (b) (6), (b) (7)(E) to this incident and issue follow-up alert A-126 to record these systems as being non-incidents. m.



200141309

General Information

Record Number:	200141309	**Center:**	ARC
Title:	Supercomputer Root Compromise (amalthea, time, Lou, touring, Helios1)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	ARC	**Coordinator:**	
Incident Category:	Unauthorized Access	**Est. Cost ($):**	1130450
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	Unknown
		Contact Email:	(b) (6), (b) (7)(C) nasa.gov
		Source of Report:	
		Est. Cost (hours):	11304.5

Incident Dates

Incident Date:	5/19/2004	**Incident Zone:**	PDT
Discovered Date:	5/19/2004	**Discovered Zone:**	PDT
NASIRC Notified Date:	5/21/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	10/12/2005	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	5/20/2004	**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:	5/19/2004	**CSO Zone:**	
OIG Date:	5/20/2004	**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	510

PII Information



SENSITIVE BUT UNCLASSIFIED

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			SGI		IRIX							IN	Account - User	7724		N/^	CAT 1



							User Compromise
(b) (6), (b) (7)(E)	SGI	IRIX	IN	Account - User	7725	N/^	CAT 1

									User Compromise
(b) (6), (b) (7)(E)	SGI	IRIX	Development	IN	Account - User	7726		N/A	CAT 1



								User Compromise
(b) (6), (b) (7)(E)	SGI	IRIX	Development	IN	Account - User	7727	N/A	CAT 1

							User Compromise
(b) (6), (b) (7)(E)	SGI	IRIX	A	Local Root Exploit	7764	N/ ^	CAT 1 U n



									User Compromise
(b) (6), (b) (7)(E)	SGI	IRIX	Workstation	SSX	Account - User	8970		N/^	CAT 1

								User Compromise
(b) (6), (b) (7)(E)	Hewlett Packard	HP-UX	Workstation	SSX	Account - User	8972	N/^	CAT 1

User Compromise

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	42070
	42071
	42072
	42077
	42197
	42059
	42060
	42061

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-138	NASIRC	3302	21-MAY-2004
A-04-138-A	NASIRC	3500	12-NOV-2004
A-04-138-B	NASIRC	3509	24-NOV-2004
A-04-138-C	NASIRC	3510	01-DEC-2004
A-04-138-D	NASIRC	4603	10-MAR-2005
A-04-138-E	NASIRC	4604	11-MAR-2005
A-04-138-F	NASIRC	4602	12-OCT-2005
USCERT#870831	CERT Team	3511	01-DEC-2004

Summary: 10/12/2005: 200141309 & 200141486 should have been combined. Please reference both. ((b) (6), (b) These two systems are currently isolated and under investigation. Block all MIT user access to turing.nas.nasa.gov.

Chronology:

Time: The wtmp on time shows a root login from amalthea.arc on 5/21 at 4:56am which was unauthorized. The logs on the system show a rshd execution as root of "sh -i" at 4:55am, then a root "rcp -t /usr/bin" at 4:55, and a root rlogin at 4:56am. A binary called zap was found in /usr/bin timestamped 4:55 which had been rcp d in from amalthea. The mtime on /etc/shadow was 5/21 at 4:56am, and it was found that a password had been added to the normally locked sysadm account at that time. A .sh_history owned by root was found in / containing commands such as "zap root" which uses his tool to erase root s login and "ssh sysadm@localhost id" to verify his sysadm root backdoor. It also contained "rm /etc/hosts.deny". Friday, Nov. 12th, 2004 - In response from (b) (6), (b) (7)(C) message "Delivered-To: (b) (6), (b) (7)(C) hq.nasa.gov X-Envelope-From: (b) (6), (b) (7)(C) ncsa.uiuc.edu Date: Fri, 12 Nov 2004 01:07:31 -0600 From: (b) (6), (b) (7)(C) To: nasirc@nasirc.hq.nasa.gov, (b) (6), (b) (7)(C) asa.gov Cc: (b) (6), (b) (7)(C) Subject: another hit User-Agent: (b) (6), (b) 1.2i X-NCSA-MailScanner-Information: Please contact the help@ncsa.uiuc.edu for more information X-NCSA-MailScanner: Found to be clean Hate to always be the bearer of bad news, but might have another hot one for you. The following was downloaded today: >198.9.15.21 - - [11/Nov/2004:09:30:30 -0500] "GET /openssh-3.7.1p2.tar.gz HTTP/1.0" 200 792723 [turing.nas.nasa.gov] That s all (from NASA at least :). (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) Head of Security Operations and Incident Response National Center for Supercomputing Applications Voice : (b) (6), (b) (7)(C) East Springfield Avenue Champaign, IL 61820 Cell : (b) (6), (b) (7)(C) http://www.ncsa.uiuc.edu/ (b) (6), (b) (7)(C) Fax : (b) (6), (b) (7)(C) -- (b) (6), (b) (7)(C), Special Agent Phone: (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) Computer Crimes Division Fax: (818) 393-3000 Western Region Cell: (b) (6), (b) (7)(C) NASA Office of Inspector General 24 HR: (818) 354-0160 " Per NAS facility investigation: It has been confirmed that a user account at MIT has been compromised. User (b) (6), (b) (7)(C). Noticed SETUID programs.. All MIT user accounts have been disabled for now. Tuesday, November 16, 2004 Per NAS (b) (6), (b) (7)(C) reported, user account (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) of MIT accessed Turing. (b) (6), (b) (7)(C) - 11/05/04 12:42 UTC from IP (b) (6), (b) (7)(E) sea.mit.edu and IP 1(b) (6), (b) (7)(C) fjord.mit.edu. (b) (6), (b) (7)(C) - 11/05/04 20:24 UTC from IP (b) (6), (b) (7)(C) swamp.mit.edu Also access attempts from (b) (6), (b) (7)(C) and (b) (6), (b). sannino - 09/07/04 09:25 UTC from IP (b) (6), (b) (7)(C) nat-75-158.casaccia.enea.it. sannino - 09/10/04 06:44 UTC from IP (b) (6), (b) (7)(C) iciv0.casaccia.enea.it. ******************************** -----Original Message----- From: US-CERT [mailto:soc@us-cert.gov] Sent: Wednesday, December 01, 2004 10:58 AM To: bulletin@nasirc.hq.nasa.gov Cc: NASIRC; soc@us-cert.gov Subject: (NASIRC Ref: 107462433) Re: (High:SGI IRIX) [NASIRC A-04-138-C] US-CERT has recieved your incident report and has been assigned USCERT#870831 for future reference. Thank you for your report, US-CERT Security Operations Center 888-282-0870 soc@us-cert.gov www.us-cert.gov ACL -- Templar / Camelot Incident - 3/7/2005 Summary: Two machines on the private network and one machine at the NAS had user level compromises on 2/23/2005. (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) from UIUC contacted us and let us know that a system known as Templar could have been compromised recently. I examined the system on 3/4/2005, and found that the dgomez account was illegally accessed on 2/23/05 at 3:32am from a machine called verlet.stanford.edu. On 2/23/05, from 3:32am until 3:43am, the attacker was logged in. From 3:34am until 3:37am, the attacker used the same pa ssword as Templar used to access Camelot.arc.nasa.gov. On Templar the history file was deleted, but on Camelot, the attacker forgot to remove his history file, allowing us to see the commands he entered. Analysis of the file system confirmed that the commands in the history were an accurate representation of the activities performed on the system by the intruder. On Templar, not much evidence of the break in was left. There was the wtmp entry, which stated: (b) (6), (b) (7)(C) verlet.stanford.edu Wed Feb 23 03:32 - 03:43. A file in (b) (6), (b) (7)(C) home directory, ssh.a.scr was last read on 2/23/2005 at 3:37am. On Camelot, the following wtmp entry was left: (b) (6), (b) (7)(C) templar.arc.nasa.gov Wed Feb 23 03:34 - 03:37 In (b) (6), (b) (7)(C) on Camelot, a .history file was left with an mtime of 2/23/2005 at 3:37am. The last part of this .history file contains the attackers commands. Also on Camelot, a authorized_keys and authorized_keys2 file was left at 3:36am. The key put into these files is a backdoor allowing remote access to the dgomez account. The atimes on the authorized_keys files matched the mtimes, indicating that the backdoor had never been used. On both Camelot and Templar, the compilers had been used to build nfsshell.tar.gz, which was run in an attempt to exploit more NFS servers on the private network. The tool was downloaded using a HTTP request via wget from www.cs.vu.nl. Lou.nas.nasa.gov was accessed briefly via the (b) (6), (b) (7)(C) account on 2/23/2005 at 3:39am. There are no signs in of this unauthorized access in (b) (6), (b) (7)(C) on Lou. Since the machine verlet.stanford.edu was the source of the attacks and was located nearby physically, I had the admin bring it to Ames to see if there was any additional evidence there. It was apparent that Verlet had been root compromised - The logs had been edited to remove the intruders entries, but there were also connections from root@127.0.0.1 at the same time that the ssh client was patched, confirming that the intruder was logged in at the time. A ls -l of /usr/bin/ssh showed a mtime in 2003, but the ctime of 2/22/2005 at 6:34am. It is almost certain that the patched ssh was installed on 2/22, one day before Templar, Camelot, and Lou were accessed. (b) (6), (b) (7)(C) also used his Columbia account from the compromised host. The ssh binary was recovered and is included with this report. Also included is the .history which was recovered, and some ls output showing that some files were accessed at 3:30 in the morning on 2/23/05. Based on the commands executed, time of day, and familiar modus operandi, it appears that the attacker is Stakkato.



NASIRC Notes:	10/12/2005: 200141309 & 200141486 should have been combined. Please reference both. ((b) (6), (b) 6/4/04: Contacted (b) (6), (b) (7)(C) regarding the addition of amalthea, time and turing to this record. He said that investigation is going on and as more information is available it will be added he said he did not enter this. (I told him I called him as the record has his name on it.) NASIRC will wait a while before updating the alert A-04-138 to allow more information to be entered. m. 07/19/2004: (b) (6), (b) (7)(C) approved an extension request from (b) (6), (b) (7)(C). The email request and approval emails can be found in the complete folder. (b) (6), (b) 11/16/2004: (b) (6), (b) (7)(E) sensors2.gsfc.nasa.gov was deleted as a hostile site. ((b) (6), (b



200141312

General Information

Record Number:	200141312	**Center:**	ARC
Title:	Misconfigured NFS		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	ARC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Other IT Concerns	**Est. Cost ($):**	7400
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:	A directory was created under a user on May 20 17:20 with Stakkato_was_here. The partition was later found to be world writable.		
		Impact:	Low
		Contact Email:	(b) (6), (b) (7)(C)nasa.gov
		Source of Report:	
		Est. Cost (hours):	74

Incident Dates

Incident Date:	5/20/2004	**Incident Zone:**	PDT
Discovered Date:	5/21/2004	**Discovered Zone:**	PDT
NASIRC Notified Date:	5/25/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	6/30/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	5/21/2004	**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:	5/21/2004	**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Software)	Sun (Hardware)	Solaris 7	Sun						SGE		7758			

Hostile Site Information

IP Address	hostile_site_id
0.0.0.0	41919

Additional Information

Notices

ID	Abbreviation	noticeid	Date
No Records Found			

Summary: Reeneabled restriction on shared partitions.

Chronology:	On May 21, 2004 the system admin has notified IT Security regarding a malicious directory, "stakkato_was_here", was created on their system. After the console review and investigation, IT Security determined that this system was not compromise other than a misconfigured NFS. The system admin might have accidentially enabled two world writable partition which allowed anyone to mount the partition and created this directory. Also, the malicious directory was created under a non privillege user. No evidience found to support that the system was compromised. Kosmos: On April 29, 2004 at 15:43, the system administrator accidently shared two directories to everyone using the Solaris share command. On 5/20 at 17:19, an attacker mounted /mnt3 and created two empty directories - One named x and the other stakkato_was_here. No other files were read or written to during that time period, and the directories were unmounted at 17:21. There is no sign of unauthorized OS access to this system, and no way to determine which system mounted the drive. Inmon did not show which system mounted the drive, probably because this system is connected to the same switch that other compromised systems were connected to, so traffic from the (b) (6), (b) (7)(E) .x subnet does not have to flow through any distributor switch or traffic logging device.
NASIRC Notes:	6/4/04: Called (b) (6), (b) (7)(C) as the information entered indicates this is a Stakkato event, however, it is listed as an Other ITS Concern. He said he didn t know what to call it as it wasn t a system compromise or user, even though under a "user a directory was created on May 20 17:20 with Stakkato_was_here." The partition was later found to be world writable. I told (b) (6), (b) (7 that the NASA community would not be seeing this event related to Stakkato as an alert as we don t issue alerts for Other ITS Concerns. (b) (6)

200141324

General Information

Record Number:	200141324	**Center:**	ARC
Title:	Supercomputer User Compromise		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	ARC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	2000
Attacker:	Stakkato/stkto	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C)asa.gov
		Source of Report:	
		Est. Cost (hours):	20

Incident Dates

Incident Date:	5/20/2004	**Incident Zone:**	PST
Discovered Date:	5/24/2004	**Discovered Zone:**	PST
NASIRC Notified Date:	6/3/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	1/19/2005	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	210

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Linux		Linux							A	Account - User	7757		N/^	CAT 1 U

							User Compromise
(b) (6), (b) (7)(E)	Linux	Linux	A	Account - User	7761	N/ ^	CAT 1 U

User Compromise

(b) (6), (b) (7)(E)	Linux	Linux	A	Account - User	7762	N/ ^	CAT 1 U

							User Compromise
(b) (6), (b) (7)(E)	Linux	Linux	A	Account - User	7763	N/ ^	CAT 1 U ~

User Compromise

Hostile Site Information

IP Address	hostile_site_id
0.0.0.0	42132

Additional Information

Notices

ID	Abbreviation	noticeid	Date
No Records Found			

Summary:

CVD: An unauthorized access occurred under the username shull from (b) (6), (b) (7)(E). The login lasted two minutes and very few files on this system had an atime last recorded between those two minutes, so very little was probably accessed. /scr2/LOGS/maillog shows a sshd connection inbound using Rhosts / RSA Authentication from (b) (6), then a telnetd connection from localhost a minute later, and a refused sshd connection 3 minutes later from (b) (6), (b) (7)(E). No backdoors or sign of root compromise was found. =============== Several systems on the private were accessed without authorization via SSH on 5/20 and 5/21. The breakins took advantage of SSH keys which were not locked with a password, allowing access from trusted machines. (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E) were compromised, and the attacker switched to several accounts in order to leverage trust relationships with machines on the private network. The systems I have looked at so far did not appear to have root level compromises, probably because all OS patches were up to date. The attacker uses the following hidden directories: ... and ,. located in / and /tmp. He attempts to delete them when he is finished, but sometimes forgets. He also sometimes forgets to remove his .sh_history, which provided some useful information. On (b) (6), (b) (7)(E), the account of (b) (6), (b) (7)(C) was compromised from (b) (6), (b) (7)(E) and touring.nas.nasa.gov. The attacker logged in to (b) (6), (b) (7)(E) at the same time the real (b) (6), (b) (7)(C) was logged in. The .sh_history file shows that the attacker was using the command "klist" to list any active kerberos tickets. These tickets are created with a SecureID card and used to log into classified Department of Defense supercomputers. After a recent compromise, the Department of Defense changed the Kerberos tickets to last only 5 minutes instead of ten hours. The attacker was checking who was idle on the system with w frequently, and if he saw activity he would run klist to see if any valid kerberos tickets could be abused. The attacker would also look at /etc/kr* for kerberos configuration information. Since the attacker was using the same source IP as the actual user and was logged in at the same time, it is difficult to determine which logins were authorized. There is however solid evidence that several of the connections were unauthorized. The attacker gains access to systems mostly by leveraging trust relationships between machines. He determined these by looking at /etc/hosts.equiv, /etc/hosts.allow, users .rhosts files, and users .ssh/known_hosts files, as well as watching where currently logged in users were connecting to. He uses a tool called "nfsshell" which exploits known weaknesses in the NFS protocol to compromise and steal files from NFS servers, and also scans the local network for samba vulnerabilities. He installed a log wiper in /usr/bin/zap and a local root backdoor in /usr/bin/foosh. Often he erases logs entirely once obtaining root access. Many of the compromised systems received connections from (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E). After we had blocked inbound SSH, he verified that it was still blocked by making inbound ssh connections from (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E).

Chronology:

CVD: An unauthorized access occurred under the username shull from (b) (6), (b) (7)(E). The login lasted two minutes and very few files on this system had an atime last recorded between those two minutes, so very little was probably accessed. /scr2/LOGS/maillog shows a sshd connection inbound using Rhosts / RSA Authentication from lou, then a telnetd connection from localhost a minute later, and a refused sshd connection 3 minutes later from (b) (6), (b) (7)(E). No backdoors or sign of root compromise was found. =============== Several systems on the private were accessed without authorization via SSH on 5/20 and 5/21. The breakins took advantage of SSH keys which were not locked with a password, allowing access from trusted machines. (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E) were compromised, and the attacker switched to several accounts in order to leverage trust relationships with machines on the private network. The systems I have looked at so far did not appear to have root level compromises, probably because all OS patches were up to date. The attacker uses the following hidden directories: ... and ,. located in / and /tmp. He attempts to delete them when he is finished, but sometimes forgets. He also sometimes forgets to remove his .sh_history, which provided some useful information. On apm-iris3, the account of (b) (6), (b) (7)(C) was compromised from (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E). The attacker logged in to apm-iris3 at the same time the real (b) (6), (b) (7)(C) was logged in. The .sh_history file shows that the attacker was using the command "klist" to list any active kerberos tickets. These tickets are created with a SecureID card and used to log into classified Department of Defense supercomputers. After a recent compromise, the Department of Defense changed the Kerberos tickets to last only 5 minutes instead of ten hours. The attacker was checking who was idle on the system with w frequently, and if he saw activity he would run klist to see if any valid kerberos tickets could be abused. The attacker would also look at /etc/kr* for kerberos configuration information. Since the attacker was using the same source IP as the actual user and was logged in at the same time, it is difficult to determine which logins were authorized. There is however solid evidence that several of the connections were unauthorized. The attacker gains access to systems mostly by leveraging trust relationships between machines. He determined these by looking at /etc/hosts.equiv, /etc/hosts.allow, users .rhosts files, and users .ssh/known_hosts files, as well as watching where currently logged in users were connecting to. He uses a tool called "nfsshell" which exploits known weaknesses in the NFS protocol to compromise and steal files from NFS servers, and also scans the local network for samba vulnerabilities. He installed a log wiper in /usr/bin/zap and a local root backdoor in /usr/bin/foosh. Often he erases logs entirely once obtaining root access. Many of the compromised systems received connections from (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E). After we had blocked inbound SSH, he verified that it was still blocked by making inbound ssh connections from (b) (6), (b) (7)(E) and (b) (6), (b) (7)(E)

NASIRC Notes:

07/19/2004: (b) (6), (b) (7)(C) approved an extension request from (b) (6), (b) (7)(C). The email request and approval emails can be found in the complete folder. (LS)



200141359

General Information

Record Number:	200141359	**Center:**	JPL
Title:	Unauthorized Access of helios.jpl.nasa.gov (JPL ID 140)		
Contact Name:	(b) (6), (b) (7)(E)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(E)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	1200
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C)nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	12

Incident Dates

Incident Date:	7/11/2004	**Incident Zone:**	PDT
Discovered Date:	7/15/2004	**Discovered Zone:**	PDT
NASIRC Notified Date:	7/15/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	9/29/2004	**Closed Zone:**	EDT

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info ?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Software)		Solaris 2.6				132				Account - User	7832		PUB	

Hostile Site Information

IP Address	hostile_site_id
 (b) (6), (b) (7)(E)	41957

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-168	NASIRC	3376	15-JUL-2004
HELIOS-ID140-07-2004	Center	3312	15-JUL-2004
JPL ID 140	Center	3440	09-SEP-2004

Summary: 9/28: (b) (6), (b) (7)(C) listed this incident in the closed section of JPL s weekly update. (b)

Chronology:	-----Original Message----- From: (b) (6), (b) (7)(C) nasa.gov [mailto:(b) (6), (b) (7)(C) nasa.gov] Sent: Thursday, July 15, 2004 1:35 PM To: jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107434727) JPL Incident Initial Notification (ID_140) INITIAL INCIDENT NOTIFICATION Investigation Name:HELIOS-ID140-07-2004 Incident Date:2004-07-11, 07:14 Investigator Name:(b) (6), (b) (7)(C) Notified By:NASIRC JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1.(b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 2.6 (5.6) | n/a | UA | User Account | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Tucson | AZ | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None.
NASIRC Notes:	



200141374

General Information

Record Number:	200141374	**Center:**	JPL
Title:	Unauthorized Access of Five JPL Systems (JPL ID 142)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	2400
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C)nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	24

Incident Dates

Incident Date:	7/20/2004	**Incident Zone:**	
Discovered Date:	7/20/2004	**Discovered Zone:**	
NASIRC Notified Date:	7/21/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	9/30/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Software)		Solaris 2.6				69				Account - User	8363		BRT	
			Redhat		Linux 7.x				132				Account - User	8364		BRT	
			Redhat		Linux 7.x				71				Account - User	8365		BRT	
			Redhat		Linux 9.x				132				Account - User	8366		BRT	
			Redhat		Linux 9.x		Workstation		132				Account - User	8098		BRT	

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41970
(b) (6), (b) (7)(E)	41961

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-179	NASIRC	3322	21-JUL-2004
A-04-179-A	NASIRC	3377	10-AUG-2004
JPL ID 142	Center	3441	09-SEP-2004
TIU-ID142-07-2004	Center	3315	21-JUL-2004

Summary: 08/10/2004: Updated incident per weekly incident report from (b) (6), (b) (7)(C) ((b) (6), (b)

Chronology: -----Original Message----- From: (b) (6), (b) (7)(C)nasa.gov [mailto:(b) (6), (b) (7)(C)nasa.gov] Sent: Wednesday, July 21, 2004 1:56 PM To: jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C)nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107435887) JPL Incident Initial Notification (ID_142) INITIAL INCIDENT NOTIFICATION Investigation Name:TIU-ID142-07-2004 Incident Date:2004-07-20, 16:51 Investigator Name:(b) (6), (b) (7)(C) Notified By:RealSecure JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. TIU | (b) (6), (b) (7)(E) | RedHat Linux 9.x | workstation | UA | User Account | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. ADSL-66-72-48-169.DSL.CHMPIL.AMERITECH.NET | 66.72.48.169 | Urbana | IL | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C)nasa.gov] Sent: Friday, August 06, 2004 7:05 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov Subject: (NASIRC Ref: 107438083) Weekly Incident Report for 23Jul04_05Aug04 INCIDENT INFO Incident Name:TIU-ID142-07-2004 Discovery Date:20-JUL-04 Exploit Date:20-JUL-04 Labor Hours:n/a Labor Cost:n/a HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) .CHMPIL.AMERITECH.NET Hostile IP:(b) (6), (b) (7)(E) Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:69 Domain Name:(b) (6), (b) (7)(E).nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:User Account System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:132 Domain Name:(b) (6), (b) (7)(E).nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:71 Domain Name:(b) (6), (b) (7)(E).nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:132 Domain Name(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:132 -- -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C)nasa.gov] Sent: Tuesday, September 21, 2004 6:34 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov Subject: (NASIRC Ref: 107449773) Weekly Incident Report for 13Sep04_20Sep04 ** CLOSED INCIDENTS: 2 ** INCIDENT INFO Incident Name:TIU-ID142-07-2004 Discovery Date:20-JUL-04 Exploit Date:20-JUL-04 Labor Hours:24 Labor Cost:2400 HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E).nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Una uthorized Access Exploit Used:User Account System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:69 Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:User Account System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:132 Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 7.x OS Version:n/a System Security Plan:71 Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 2.6 (5.6) OS Version:n/a System Security Plan:132 Domain Name:(b) (6), (b) (7)(E).nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:132

NASIRC Notes:



200141421

General Information

Record Number:	200141421	**Center:**	JPL
Title:	Unauthorized Access of Four JPL Systems (JPL ID 146)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	28400
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C)nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	284

Incident Dates

Incident Date:	8/28/2004	**Incident Zone:**	
Discovered Date:	8/28/2004	**Discovered Zone:**	
NASIRC Notified Date:	8/31/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	9/30/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Software)		Solaris 8		Unknown						Account - User	8417		N/A	
			Sun (Software)		Solaris 8								Account - User	8418		N/A	
			Sun (Software)		Solaris 7				482				Account - User	8419		N/A	
			Redhat		Linux 8.0				85				Account - User	8420		N/A	

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	41998
(b) (6), (b) (7)(E)	42000

Additional Information



SENSITIVE BUT UNCLASSIFIED

Notices

ID	Abbreviation	noticeid	Date
A-04-221	NASIRC	3401	31-AUG-2004
JPL ID 146	Center	3443	09-SEP-2004
(b) (6), (b) (7)(E) id146-08-20	Center	3382	31-AUG-2004

Summary: 09/30/2004: Closed per (b) (6), (b) (7)(C) weekly incident report. (b) (6), (b

Chronology: -----Original Message----- From: (b) (6), (b) (7)(C) nasa.gov [mailto:(b) (6), (b) (7)(C) nasa.gov] Sent: Tuesday, August 31, 2004 11:51 AM To: jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107445766) JPL Incident Initial Notification (ID_146) INITIAL INCIDENT NOTIFICATION Investigation Name:(b) (6), (b) (7)(E) Incident Date:2004-08-28, 05:51 Investigator Name:(b) (6), (b) (7)(C) Notified By:SNORT JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 9.x | Desktop workstation | SC | Local Root Exploit | No | None 2. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 8 (2.8) | desktop workstation | UA | User Account | No | None 3. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 8 (2.8) | NFS server | UA | User Account | No | None 4. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 7 (2.7) | web server | UA | User Account | No | None 5. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 8.x | desktop workstation | UA | User Account | No | None 6. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 9.x | desktop workstation | SC | Local Root Exploit | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Lausanne | n/a | Switzerland 2. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Boulder | CO | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C) nasa.gov] Sent: Wednesday, September 29, 2004 6:18 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov Subject: (NASIRC Ref: 107452372) Weekly Incident Report for 28Sep04_28Sep04 ** CLOSED INCIDENTS: 2 ** INCIDENT INFO Incident Name:(b) (6), (b) (7)(E) ID146-08-2004 Discovery Date:28-AUG-04 Exploit Date:28-AUG-04 Labor Hours:284 Labor Cost:28400 HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E) nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E) nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E) nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E) nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 7 (2.7) OS Version:n/a System Security Plan:482 Domain Name(b) (6), (b) (7)(E) nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 8.x OS Version:n/a System Security Plan:85 Domain Name:(b) (6), (b) (7)(E) nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a

NASIRC Notes:



200141422

General Information

Record Number:	200141422	**Center:**	JPL
Title:	System Compromise of Two JPL Systems (JPL ID 146)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	System Compromise	**Est. Cost ($):**	28400
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C) nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	284

Incident Dates

Incident Date:	8/28/2004	**Incident Zone:**	
Discovered Date:	8/28/2004	**Discovered Zone:**	
NASIRC Notified Date:	8/31/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	9/30/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Redhat		Linux 9.x		Workstation						Local Root Exploit	8416		N/A	
			Redhat		Linux 9.x								Local Root Exploit	8421		N/A	

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	42001
(b) (6), (b) (7)(E)	42002

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-04-222	NASIRC	3400	31-AUG-2004
JPL ID 146	Center	3444	09-SEP-2004
(b) (6), (b) (7)(E) id146-08-20	Center	3381	31-AUG-2004

Summary:	09/30/2004: Closed per weekly incident report from (b) (6), (b) (7)(C) @ JPL. ((b) (6), (b
Chronology:	-----Original Message----- From: (b) (6), (b) (7)(C)nasa.gov [mailto:(b) (6), (b) (7)(C)nasa.gov] Sent: Tuesday, August 31, 2004 11:51 AM To: jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C)nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107445766) JPL Incident Initial Notification (ID_146) INITIAL INCIDENT NOTIFICATION Investigation Name:(b) (6), (b) (7)(E) Incident Date:2004-08-28, 05:51 Investigator Name:(b) (6), (b) (7)(C) Notified By:SNORT JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 9.x | Desktop workstation | SC | Local Root Exploit | No | None 2. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 8 (2.8) | desktop workstation | UA | User Account | No | None 3. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 8 (2.8) | NFS server | UA | User Account | No | None 4. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 7 (2.7) | web server | UA | User Account | No | None 5. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 8.x | desktop workstation | UA | User Account | No | None 6. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 9.x | desktop workstation | SC | Local Root Exploit | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Lausanne | n/a | Switzerland 2. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Boulder | CO | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ********************************* -----Original Message----- From: (b) (6), (b) (7)(C) [mailto(b) (6), (b) (7)(C)nasa.gov] Sent: Wednesday, September 29, 2004 6:18 PM To: nasirc@nasirc.hq.nasa.gov Cc: security@telchar.jpl.nasa.gov; jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C)nasa.gov Subject: (NASIRC Ref: 107452372) Weekly Incident Report for 28Sep04_28Sep04 ** CLOSED INCIDENTS: 2 ** INCIDENT INFO Incident Name:(b) (6), (b) (7)(E) Discovery Date:28-AUG-04 Exploit Date:28-AUG-04 Labor Hours:284 Labor Cost:28400 HOSTILE SYSTEMS Hostile Name:LANOSLNX.EPFL.CH Hostile IP:128.178.34.19 Hostile Name:(b) (6), (b) (7)(E) Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:(b) (6), (b) (7)(E)jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:n/a Domain Name:(b) (6), (b) (7)(E) nasa.gov IP Address:137.78.218.98 Incident Category:Unauthorized Access Exploit Used:User Account System OS:Sun Solaris 7 (2.7) OS Version:n/a System Security Plan:482 Domain Name(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:Unauthorized Access Exploit Used:User Account System OS:RedHat Linux 8.x OS Version:n/a System Security Plan:85 Domain Name:(b) (6), (b) (7)(E)nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Local Root Exploit System OS:RedHat Linux 9.x OS Version:n/a System Security Plan:n/a
NASIRC Notes:	



200141479

General Information

Record Number:	200141479	**Center:**	JPL
Title:	helios, orac, frigg and platte (JPL ID 154)		
Contact Name:	(b) (6)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	4000
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	Medium
		Contact Email:	(b) (6), (b) (7)(C) nasa.gov
		Source of Report:	(b) (6) UIUC------RealSecure
		Est. Cost (hours):	40

Incident Dates

Incident Date:	10/22/2004	**Incident Zone:**	
Discovered Date:	10/22/2004	**Discovered Zone:**	
NASIRC Notified Date:	10/23/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	12/2/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	10/25/2004	**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			Sun (Hardware)		Solaris 9				132				Root Account Cracked	8625		SER	CAT 1 U n

							System Compromise
(b) (6), (b) (7)(E)	Redhat	Linux 7.x	245	Root Account Cracked	8627	SER	CAT 1 U n

							System Compromise
(b) (6), (b) (7)(E)	Redhat	Linux 9.x	132	Account - User	8629	SER	CAT 1



							System Compromise
(b) (6), (b) (7)(E)	Redhat	Linux 9.x	372	Root Account Cracked	8697	SER	CAT 1 U

Sys
te
m
Co
mp
ro
mis
e

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	42047

Additional Information

Notices

ID	Abbreviation	noticeid	Date
PLATTE-ID154-10-2004	Center	3483	27-OCT-2004

Summary: 10/27/2004: Received a JPL Incident Initial Notification. ((b) (6)) Alert issued. ((b) (6)) 11/19/2004: NASIRC received updated information regarding this incident. Updates were made. ((b) (6))

Chronology:	-----Original Message----- From: (b) (6), (b) (7)(C) nasa.gov [mailto:(b) (6), (b) (7)(C) nasa.gov] Sent: Wednesday, October 27, 2004 1:37 PM To: jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C) nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107456054) JPL Incident Initial Notification (ID_154) INITIAL INCIDENT NOTIFICATION Investigation Name:PLATTE-ID154-10-2004 Incident Date:2004-10-22, 12:00 Investigator Name:(b) (6), (b) (7)(C) Notified By:RealSecure JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | RedHat Linux 9.x | n/a | SC | Root account cracked | No | None 2. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 9 | n/a | SC | Root account cracked | No | None 3. ORAC | (b) (6), (b) (7)(E) | RedHat Linux 7.x | n/a | SC | Root account cracked | No | None 4. PLATTE | (b) (6), (b) (7)(E) | RedHat Enterprise 3 | n/a | SC | User Account | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. UNREGISTERED | (b) (6), (b) (7)(E) | London | n/a | United Kingdom Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ********************** -----Original Message----- From: (b) (6), (b) (7)(C) Sent: Monday, October 25, 2004 6:08 AM To: (b) (6), (b) (7)(C); (b) (6), (b) (7)(C) Subject: FW: (NASIRC Ref: 107455487) new info (fwd) Got some more info that you will probably want to look into. We are monitoring a web server that stakkato has some exploits, the suckit rootkit and his trojaned ssh client. The following was in the web logs when I checked today: (b) (6), (b) (7)(E) - - [24/Oct/2004:10:27:48 -0400] "GET /openssh-3.7.1p2.tar.gz HTTP/1.0" 200 792723 [helios.jpl.nasa.gov] (b) (6), (b) (7)(E) - - [24/Oct/2004:10:48:52 -0400] "GET /openssh-3.7.1p2.tar.gz HTTP/1.0" (b) (6), (b) (7)(E) [orac.jpl.nasa.gov] The current password collector uses the DynDNS hostname stakkato.dyndns.ws and points to (b) (6), (b) (7)(E) (aae105-dhcp-13.ecn.purdue.edu). You might want to see if you have any network flows to that host on port 53. We are working with Purdue to get more info from this machine, but it s taking a bit of time. Let me know if you need more info. (b) (6), -- (b) (6), (b) (7)(C) Head of Security Operations and Incident Response National Center for Supercomputing Applications Voice : (b) (6), (b) (7)(C) East Springfield Avenue Champaign, IL 61820 Cell : (b) (6), (b) (7)(C) http://www.ncsa.uiuc.edu/(b) (6), (b) (7)(C) Fax : (b) (6), (b) (7)(C) Date: Sat, 23 Oct 2004 01:55:02 -0500 From: (b) (6), (b) (7)(C) To: nasirc@nasirc.hq.nasa.gov,(b) (6), (b) (7)(C) nasa.gov Cc: (b) (6), (b) (7)(C) Subject: (NASIRC Ref: 107455487) new info (b) (6), (b) (7), et. al., Got some info earlier from a friend who has been watching some IRC channels for our friend and saw this pop up today: (15:38) [EFNet] -!- Irssi: stakkato [~(b) (6), (b) (7)(C) jpl.nasa.gov] [(b) (6), (b) (7)(C)] has joined to EFNet (16:17) [EFNet] -!- Irssi: stakkato has left EFNet (20:33) [EFNet] -!- stakkato [~(b) (6), (b) (7)(C).jpl.nasa.gov] (20:33) [EFNet] -!- was : (b) (6), (b) (7)(C) (20:33) [EFNet] -!- server : irc.efnet.nl [Fri Oct 22 16:16:38 2004] (20:33) [EFNet] -!- End of WHOWAS Looks like someone with the account (b) (6), (b) (7)(C) platte.jpl.nasa.gov got on EFNet with the nick of stakkato this afternoon. Not sure how they got this account, but it might be good to touch base sometime early next week and I can update you on the activity we have seen in the last few weeks (machines compromised, etc.). (b) (6), - -- (b) (6), (b) (7)(C) Head of Security Operations and Incident Response National Center for Supercomputing Applications Voice : (b) (6), (b) (7)(C) East Springfield Avenue Champaign, IL 61820 Cell : (b) (6), (b) (7)(C) http://www.ncsa.uiuc.edu/(b) (6), (b) (7)(C) Fax : (b) (6), (b) (7)(C) ------- End of Forwarded Message
NASIRC Notes:	10/27/2004: aae105-dhcp-13.ecn.purdue.edu ((b) (6), (b) (7)(E) was provided by (b) (6), (b) (7)(C) ((b) (6), (b



200141486

General Information

Record Number:	200141486	**Center:**	ARC
Title:	Compromised Account on Lomax(NAS)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	ARC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	1130450
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C)nasa.gov
		Source of Report:	
		Est. Cost (hours):	11304.5

Incident Dates

Incident Date:	10/22/2004	**Incident Zone:**	PDT
Discovered Date:	10/23/2004	**Discovered Zone:**	PDT
NASIRC Notified Date:	10/25/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	10/19/2005	**Closed Zone:**	EST

Dates For Other Notifications

ITSM Date:		**ITSM Zone:**	
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	360

PII Information



~~SENSITIVE BUT UNCLASSIFIED~~

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)			SGI	SGI	IRIX	Unknown						IN	Account - User	8639	Y	SER	CAT 1

User Compromise

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	42820

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-05-180	NASIRC	4597	20-OCT-2005

Summary: 10/12/2005: 200141309 & 200141486 should have been combined. Please reference both. ((b) (6), (b) ***Begin ARC/NAS system to watch (Incident Record # 200141478)*** lomax.nas.nasa.gov ((b) (6), (b) (7)(E)) account: (b) (6), (b) (7)(C) ***End ARC*** 10/25/2004: Received a report of a 48 hour inbound & outbound block of lomax.nas.nasa.gov ((b) (6), (b) (7)(E)) from Remedy. Email sent to (b) (6), (b) (7)(C). ((b) (6), (b)

SENSITIVE BUT UNCLASSIFIED

Chronology: Reply-To: (b) (6), (b) (7)(C)nasa.gov To: (b) (6), (b) (7)(C) Subject: Re: Recent incident From: Dave Tweten Date: Mon, 25 Oct 2004 10:34:52 -0700 Sender: (b) (6), (b) (7)(C) nas.nasa.gov X-Junkmail-Status: score=15/60, host=arc-relay2.arc.nasa.gov X-Junkmail-Whitelist: YES (by domain whitelist at arc-relay2.arc.nasa.gov) Attachment converted: Macintosh HD:Re- Recent incident (MiME/CSOm) (0022094C) On Saturday afternoon, (b) (6), (b) (7)(C) relayed a message from NISN, indicating that there was IRC traffic between lomax.nas.nasa.gov and Romania. (b) (6), (b) (7) came in and discovered a compromised user account, spahr. It is an account belonging to (b) (6), (b) (7)(C), of UCLA. (b) (6), (b) (7) said it had an IRC relay installed on Lomax, as the user. (b) (6), (b) (7)(C) also noticed evidence that other UCLA accounts may have been compromised too. We decided to disable all accounts coming to us from UCLA until we could sort things out. (b) (6), (b) (7)(C) promised to page me if anything more serious turned up, and promised to give me a full report when he comes in on Monday. I have not been paged. -- Office: (b) (6), (b) (7)(C), M/S: (b) (6), (b) (7)(C) Phone: (b) (6), (b) (7)(C), FAX: (b) (6), (b) (7)(C) 1024-bit PGP fingerprint: (b) (6), (b) (7)(C) The foregoing is far too clearly stated to be an official NASA position. *************************** -----Original Message----- From: Mail, Remedy [mailto:Remedy.Mail@msfc.nasa.gov] Sent: Saturday, October 23, 2004 8:32 PM To: nasirc@nasirc.hq.nasa.gov Subject: (NASIRC Ref: 107455509) ITS Event ITS000000070168 UNITES ENMC Assignment ITS Event ITS000000070168 has been assigned to UNITES ENMC and is blocked 48 Hours. Type of Event : UNAUTHORIZED ACCESS *************************************** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C)nasa.gov] Sent: Monday, October 25, 2004 11:10 AM To: (b) (6), (b) (7)(C) Cc: (b) (6), (b) (7)(C) (E-mail) ; (b) (6), (b) (7)(C); (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C); (b) (6), (b) (7)(C) (b) (6), (b) (7)(C); (b) (6), (b) (7)(C); (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (b) (6), (b) (7)(C); (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C)nasa.gov ; (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C)nasa.gov Subject: Re: Supercomputer Incident Update Importance: High Folks, ARC responded to NISN s notice, and found that a UCLA user account was compromised on Lomax (b) (6), (b) (7)(E) - (b) (6), (b) (7)(C) They also found a binary downloaded on Lomax, Oct. 22, 2004 that was reported to consist of the following characters: PSFLYBNZ (reported by (b) (6), (b) (7)(C) the IT Security person in charge of the NAS) ARC disabled all the UCLA user accounts from the machine. (b) (6), (b) (7)(C) At 11:37 AM -0400 10/25/04, (b) (6), (b) (7)(C) wrote: >Attachment converted: Intrigue:smime 106.p7m (MiME/CSOm) (000A96F0) > > >= = = = Security Information = = = = >Signed with SHA1-RSA >Encrypted with RC2-128 Compatible >Signed By: (b) (6), (b) (7)(C) 1 >Certified By: cn=EntrustCA, o=National Aeronautics and Space >Administration, c=US > > >Hey Gang, > >(b) (6), (b) (7)(C) reported some more possible Supercomputing Activity at >JPL after seeing some IRC traffic. Coincidentally, NISN also >blocked an NAS system around the same time because of questionable >IRC traffic to Romania. I m 99% sure the systems at JPL were hit by >you-know-who. NAS could be a coincidence. > >Here are the systems to watch out for: > >JPL (Incident Record # 200141479) >helios.jpl.nasa.gov (b) (6), (b) (7)(E)) >orac.jpl.nasa.gov ((b) (6), (b) (7)(E)) >platte.jpl.nasa.gov ((b) (6), (b) (7)(E)) >account: (b) (6), (b) (7)(C) platte.jpl.nasa.gov, (b) (6), (b) (7)(C), P hone (b) (6), (b) (7)(C), Org 3474 > >ARC/NAS (Incident Record # 200141478) >lomax.nas.nasa.gov (b) (6), (b) (7)(E)) > >University of Purdue (Incident Record # 200141479) >aae105-dhcp-13.ecn.purdue.edu ((b) (6), (b) (7)(E)) > > > >(b) (6), (b) (7) messages are attached below. > > > >Carey >Begin Fwd Msg > > >-----Original Message----- >From: (b) (6), (b) (7)(C) >Sent: Monday, October 25, 2004 6:08 AM >To: (b) (6), (b) (7)(C) (b) (6), (b); (b) (6), (b) (7)(C) >Subject: FW: (NASIRC Ref: 107455487) new info (fwd) > >Got some more info that you will probably want to look into. We are >monitoring >a web server that stakkato has some exploits, the suckit rootkit and >his trojaned ssh client. The following was in the web logs when I >checked today: > >(b) (6), (b) (7)(E) - - [24/Oct/2004:10:27:48 -0400] "GET >/openssh-3.7.1p2.tar.gz HTTP/1.0" 200 792723 >[helios.jpl.nasa.gov] >(b) (6), (b) (7)(E) - - [24/Oct/2004:10:48:52 -0400] "GET >/openssh-3.7.1p2.tar.gz HTTP/1.0" 200 792723 >[orac.jpl.nasa.gov] > >The current password collector uses the DynDNS hostname stakkato.dyndns.ws >and points to (b) (6), (b) (7)(E) (aae105-dhcp-13.ecn.purdue.edu). You might >want to see if you have any network flows to that host on port 53. We are >working with Purdue to get more info from this machine, but it s taking a bit >of time. > >Let me know if you need more info. > >(b) (6), > >-- >(b) (6), (b) (7)(C) >Head of Security Operations and Incident Response >National Center for Supercomputing Applications Voice : (b) (6), (b) (7)(C) >605 East Springfield Avenue Champaign, IL 61820 Cell : (b) (6), (b) (7)(C) >http://www.ncsa.uiuc.edu/~jbarlow Fax : (b) (6), (b) (7)(C) >Date: Sat, 23 Oct 2004 01:55:02 -0500 >From: (b) (6), (b) (7)(C) >To: nasirc@nasirc.hq.nasa.gov, (b) (6), (b) (7)(C)nasa.gov >Cc: (b) (6), (b) (7)(C) >Subject: (NASIRC Ref: 107455487) new info > >(b) (6), (b) (7)(C) et. al., > >Got some info earlier from a friend who has been watching some IRC >channels for our friend and saw this pop up today: > >(15:38) [EFNet] -!- Irssi: stakkato [~(b) (6), (b) (7)(C)jpl.nasa.gov] [(b) (6), (b) (7)(C)] has joined to EFNet >(16:17) [EFNet] -!- Irssi: stakkato has left EFNet >(20:33) [EFNet] -!- stakkato [~(b) (6), (b) (7)(C)jpl.nasa.gov] >(20:33) [EFNet] -!- was : (b) (6), (b) (7)(C) >(20:33) [EFNet] -!- server : irc.efnet.nl [Fri Oct 22 16:16:38 2004] >(20:33) [EFNet] -!- End of WHOWAS > >Looks like someone with the account (b) (6), (b) (7)(C)jpl.nasa.gov got >on EFNet with the nick of stakkato this afternoon. Not sure how they >got this account, but it might be good to touch base sometime early next >week and I can update you on the activity we have seen in the last few >weeks (machines compromised, etc.). > >(b) (6), (b) > >- -- >(b) (6), (b) (7)(C) Barlow >Head of Security Operations and Incident Response >National Center for Supercomputing Applications Voice : (b) (6), (b) (7)(C) >605 East Springfield Avenue Champaign, IL 61820 Cell : (b) (6), (b) (7)(C) >http://www.ncsa.uiuc.edu/(b) (6), (b) (7)(C) Fax : (b) (6), (b) (7)(C) > >------- End of Forwarded Message >Content-Type: application/rtf > >Attachment converted: Intrigue:Untitled 95 (????/----) (000A9755) -- (b) (6), (b) (7)(C) Office phone



(b) (6), (b) (7)(C) NASA Ames Research Center Cell: (b) (6), (b) (7)(C) Center Information Technology Security Manager (ITSM) Home Cell: (b) (6), (b) (7)(C). Office of the Chief Information Officer MS 233-17 NASA ARC (b) (6), (b) (7)(C)nasa.gov Moffett Field, CA 94035 ======================= Subject: Re: Fwd: FW: (NASIRC Ref: 0003115) Incidents 200141486 and 200141309 From: "(b) (6), (b) (7)(C)" Reply-To: (b) (6), (b) (7)(C)nasa.gov To: (b) (6), (b) (7)(C) Organization: NASA Advanced Supercomputing Division Date: Wed, 19 Oct 2005 16:39:10 -0700 X-Proofpoint-Spam-Reason: safe Operating System: SGI Irix Version Number: 6.5.23 Exploit Type: User account password compromise at UCLA Information Category: non-sensitive SER Date/Time of Discovery: 1641PDT Oct 23, 2004 Date/Time of Exploit: 1521PDT Oct 22, 2004 Hostile Site: (b) (6), (b) (7)(E)

NASIRC Notes:	10/12/2005: 200141309 & 200141486 should have been combined. Please reference both. ((b) (6), (b 10/26/2004: (b) (6), entered 200141478 on 10/25/2004, ARC entered 200141486. (b) (6), (b copied information from 200141478 summary and pasted into 200141486. 11/23/2004: (b) (6), (b) (7)(C) approved an extension for this incident ((b) (6), (b -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C) nasa.gov] Sent: Tuesday, November 23, 2004 2:40 PM To: (b) (6), (b) (7)(C) Cc: (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(C); (b) (6), (b) (7)(C) nasa.gov; (b) (6), (b) (7)(Subject: Re: Fwd: RE: Waivers for 30 Incident Close-out approved... M



200141493

General Information

Record Number:	200141493	**Center:**	GSFC
Title:	Linux kernel Exploit of Three GSFC Systems		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	2600
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	Unknown
		Contact Email:	(b) (6), (b) (7)(C)nasa.gov
		Source of Report:	(b) (6), (b) (7)(C) UIUC
		Est. Cost (hours):	26

Incident Dates

Incident Date:	11/6/2004	**Incident Zone:**	EST
Discovered Date:	11/6/2004	**Discovered Zone:**	EST
NASIRC Notified Date:	11/6/2004	**NASIRC Notified Zone:**	EDT
Closed Date:	12/10/2004	**Closed Zone:**	

Dates For Other Notifications

ITSM Date:	11/8/2004	**ITSM Zone:**	EST
US-CERT Date:		**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:		**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:		**CCITS Zone:**	
		Time Limit:	30

PII Information



SENSITIVE BUT UNCLASSIFIED

PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)		Richard Molle	Linux	Mandrake	Other	Unknown	Server: Application					900.3	Linux Kernel do_brk	8713		SER	CAT 6 Investigations
(b) (6), (b) (7)(E)			SGI		IRIX		Workstation					913		8790		SER	CAT 1 U

User Compromise

(b) (6), (b) (7)(E)

8792

CAT 1

Un

User Compromise

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	42091

Additional Information

Notices

ID	Abbreviation	noticeid	Date
107458683	Mail Handler	3489	06-NOV-2004

Summary: 11/06/04: (b) (6), (b) (7)(C) sent an email on this Saturday to NASIRC notifying us that the password collector moved and that cerebus may be hacked. ci. 11/08/04: (b) (6), (b) (7)(found the email this morning (Monday) and fwd to group. (b) (6), (b) called and said this was compromised and that other systems may also be affected. (b) (6), (b) (is looking into it and we can anticipate a report tomorrow. ci. 11/09/04: (b) (6), (b) (7) added the traffic captured by NISN and fwd to group. (b) (6), (b) (7 confirmed what (b) (6), (b) said yesterday, and we can still anticipate a report later today. ci. 12/10/2004: This system has returned to operation. Incident hours updated. 12/15/2004: Incident hours updated.



Chronology:

-----Original Message----- From: (b) (6), (b) (7)(C) Sent: Monday, November 08, 2004 8:25 AM To: (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) (E-mail) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) (E-mail) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) nasa.gov ; (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) nasa.gov Cc: (b) (6), (b) (7)(C) ; (b) (6), (b) (7)(C) (b) (6), (b) (7)(C) (E-mail) ; (b) (6), (b) (7)(C) (E-mail) Subject: update Importance: High ***** ADMINISTRATIVELY CONTROLLED INFORMATION ***** ***** ENCRYPT PRIOR TO TRANSMISSION ***** Hi Gang, (b) (6), (b) (7)(C) suspects cerebus.gsfc.nasa.gov has been hacked. He also reports the password collector has moved to pacbell.net. My queries on NCARS IDS data for a one month interval on both of these IP addresses yield a null result. (Incident 200141493 has been opened as an Unconfirmed Report for cerebus.) (b) (6), (b) (7) -----Original Message----- From: (b) (6), (b) (7)(C) [mailto (b) (6), (b) (7)(C) ncsa.uiuc.edu] Sent: Saturday, November 06, 2004 11:52 PM To: nasirc@nasirc.hq.nasa.gov; (b) (6), (b) (7)(C) nasa.gov Cc: (b) (6), (b) (7)(C) Subject: (NASIRC Ref: 107458683) another host Got another host to track down. The following was downloaded from the web server that we are monitoring: (b) (6), (b) (7)(E) - - [06/Nov/2004:08:08:47 -0500] "GET /.mremap_pte HTTP/1.0" 200 467647 [cerebus.gsfc.nasa.gov] The above is a precompiled linux kernel exploit. Another thing to note is that the password collector moved this morning to (b) (6), (b) (7)(E) (adsl-67-125-72-209.dsl.snfc21.pacbell.net). That s all I got for now. (b) (6), -- (b) (6), (b) (7)(C) Head of Security Operations and Incident Response National Center for Supercomputing Applications Voice : (b) (6), (b) (7)(C) 605 East Springfield Avenue Champaign, IL 61820 Cell : (b) (6), (b) (7)(C) http://www.ncsa.uiuc.edu/ (b) (6), (b) (7)(C) Fax : (b) (6), (b) (7)(C) ***BEGIN NISN CAPTURE*** 07:08 CDT 11-06-2004 IP (b) (6), (b) (7)(E) makes contact with (b) (6), (b) (7)(E) via port 53 (DNS). Although there is no full packet capture, ensuing traffic does not resemble "normal"* DNS traffic: * "normal" DNS traffic usually uses the UDP protocol, although it can use TCP. However, the DNS name of (b) (6), (b) (7)(E) (ads (b) (6), (b) (7)(E) .dsl.snfc21.pacbell.net) indicates a DSL connection, which makes it unlikely to have a valid DNS server running. 07:08:25.691611 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) : S (b) (6), (b) (7)(E) : (b) (6), (b) (7)(E) (0) win 5840 (DF) [tos 0x10] 07:08:27.057543 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) : S (b) (6), (b) (7)(E) : (b) (6), (b) (7)(E) (0) ack (b) (6), (b) (7)(E) win 5792 (DF) [tos 0x10] 07:08:27.058293 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) . ack 1 win 5840 (DF) [tos 0x10] 07:08:29.200389 (b) (6), (b) (7)(E) > 67.125.72.209.53: P 1:9(8) ack 1 win 5840 (DF) [tos 0x10] 07:08:29.299075 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) . ack 9 win 5792 (DF) [tos 0x10] 07:08:29.520690 (b) (6), (b) (7)(E) > 67.125.72.209.53: P 9:17(8) ack 1 win 5840 (DF) [tos 0x10] 07:08:29.620507 67.125.72.209.53 > (b) (6), (b) (7)(E) : . ack 17 win 5792 (DF) [tos 0x10] 07:08:29.620881 67.125.72.209.53 > (b) (6), (b) (7)(E) : F 1:1(0) ack 17 win 5792 (DF) [tos 0x10] 07:08:29.621631 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) : F 17:17(0) ack 2 win 5840 (DF) [tos 0x 10] 07:08:29.720823 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) : . ack 18 win 5792 (DF) [tos 0x10] 07:08:36 CDT IP 128.183.107.95 connects to 66.92.150.48 (lick.myleft.net) via port 80, and begins transfer of data. Though we do not have any payload data, the timestamp and connection characteristics are consistent with the details of the compromise. 07:08:36.965855 128.183.107.95.48884 > (b) (6), (b) (7)(E) S (b) (6), (b) (7)(E) : (b) (6), (b) (7)(E) (0) win 5840 (DF) 07:08:37.146247 (b) (6), (b) (7)(E) (b) (6), (b) (7)(E) : S (b) (6), (b) (7)(E) : (b) (6), (b) (7)(E) (0) ack 1342853138 win 32120 (DF) 07:08:37.147121 (b) (6), (b) (7)(E) > 66.92.150.48.80: . ack 1 win 5840 (DF) 07:08:37.147371 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) : P 1:111(110) ack 1 win 5840 (DF) 07:08:37.327513 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) . ack 111 win 32120 (DF) 07:08:37.425955 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) : P 1:1449(1448) ack 111 win 32120 (DF) 07:08:37.427086 (b) (6), (b) (7)(E) > 66.92.150.48.80: . ack 1449 win 8688 (DF) 07:08:37.459808 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) P 1449:2897(1448) ack 111 win 32120 (DF) 07:08:37.461058 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) . ack 2897 win 11584 (DF) ... 07:08:49.044617 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) F 111:111(0) ack 467956 win 63712 (DF) 07:08:49.222013 66.92.150.48.80 > (b) (6), (b) (7)(E) . ack 112 win 32120 (DF) 07:08:49.224133 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) F 467956:467956(0) ack 112 win 32120 (DF) 07:08:49.224759 (b) (6), (b) (7)(E) > (b) (6), (b) (7)(E) . ack 467957 win 63712 (DF) 07:13 CDT IP (b) (6), (b) (7)(E) connects to (b) (6), (b) (7)(E) (login.hpcx.ac.uk) via port 22 (SSH), transfers some data, then connects to (b) (6), (b) (7)(E) (soling.cs.vu.nl) via port 80. Because we have no full packet captures, any traffic listed by this point is debatable as to if it is "normal" or hostile traffic. No further outbound traffic is seen coming from (b) (6), (b) (7)(E) for the rest of the day. ***END NISN CAPTURE***

NASIRC Notes:



200141547

General Information

Record Number:	200141547	**Center:**	JPL
Title:	Unauthorized Access of tcom-cm-out.jpl.nasa.gov ((b) (6), (b) (7)(E)) (ID160)		
Contact Name:	(b) (6), (b) (7)(C)	**Contact Phone:**	
Contact Center:	NASIRC	**Coordinator:**	(b) (6), (b) (7)(C)
Incident Category:	Unauthorized Access	**Est. Cost ($):**	1400
Attacker:	Stakkato	**Hostile Unknown?:**	No
Attacker Note:			
		Impact:	High
		Contact Email:	(b) (6), (b) (7)(C) nasirc.nasa.gov
		Source of Report:	(b) (6), (b) (7)(C)
		Est. Cost (hours):	14

Incident Dates

Incident Date:	2/22/2005	**Incident Zone:**	EST
Discovered Date:	2/22/2005	**Discovered Zone:**	
NASIRC Notified Date:	2/22/2005	**NASIRC Notified Zone:**	EST
Closed Date:	3/6/2005	**Closed Zone:**	EST

Dates For Other Notifications

ITSM Date:	2/22/2005	**ITSM Zone:**	
US-CERT Date:	2/22/2005	**US-CERT Zone:**	
CSO Date:		**CSO Zone:**	
OIG Date:	2/22/2005	**OIG Zone:**	
CIO Date:		**CIO Zone:**	
ITSO Date:		**ITSO Zone:**	
CCITS Date:	2/22/2005	**CCITS Zone:**	
		Time Limit:	30

PII Information



PII Involved?:	No	**PII Report Date:**	
PII Disclosed By:		**PII Data Protection:**	Unknown
PII Data Types:			
Scope of PII Exposure:		**Number of Unauthorized People with Access:**	
		PII Report Zone:	
		Law Enforcement/ IG Notified?:	No

Host Information

NASA System Information

Name	IP Address	Admin	OS Manufacturer	HW Manufacturer	OS Version	HW Version	Function	Sensitivity Description	Security Plan	CVE	Port	Org. Code	Exploit	system_id	Sensitive Info?	Information Category	Category
(b) (6), (b) (7)(E)		168	Sun (Software)		Solaris 8		Server: Harvest						Root Account Cracked	8936		SER	CAT 1 U

Sys
te
m
Co
mp
ro
mis
e

Hostile Site Information

IP Address	hostile_site_id
(b) (6), (b) (7)(E)	42188

Additional Information

Notices

ID	Abbreviation	noticeid	Date
A-05-38	NASIRC	3573	22-FEB-2005
A-05-38-A	NASIRC	3572	07-MAR-2005
TCOM-CM-OUT-ID160	Center	3567	22-FEB-2005

Summary:	2/22: (b) (6), (b) (7)(C) supplied NASA with some information via phone and email about a Stakkato incident. (b) (6), (b) (7) called (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) at JPL. They were aware of the activity and were already conducting analysis. (b) (6), (b) (7) left voice mail for (b) (6), (b) (7)(C) and (b) (6), (b) (7)(C) apprising them of the situation. Called (b) (6), (b) (7)(C) also but did not leave a message because his greeting said he was out of the office. Then sent (b) (6), (b) (7) email to the FRT group of old. (b) (6), (b) (b) (6), (b) (7)(C) certificate was expired so he was removed from the distribution. Called him instead and he was already up to speed. - ci.
Chronology:	-----Original Message----- From: (b) (6), (b) (7)(C).jpl.nasa.gov [mailto:(b) (6), (b) (7)(C).jpl.nasa.gov] Sent: Tuesday, February 22, 2005 4:19 PM To: jpl-ccd@imx.hq.nasa.gov; (b) (6), (b) (7)(C).jpl.nasa.gov; (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C)jpl.nasa.gov; nasirc@nasirc.hq.nasa.gov; security@telchar.jpl.nasa.gov Subject: (NASIRC Ref: 107485899) JPL Incident Initial Notification (ID_160) INITIAL INCIDENT NOTIFICATION Investigation Name:TCOM-CM-OUT-ID160-02-2005 Incident Date:2005-02-22, 08:00 Investigator Name:(b) (6), (b) (7)(C) Notified By:SNORT JPL Computer Information: HOSTNAME | IP ADDRESS | OS | FUNCTION | INCIDENT CAT | EXPLOIT | SENS INFO | SENS INFO DESC 1. (b) (6), (b) (7)(E) | (b) (6), (b) (7)(E) | Sun Solaris 8 (2.8) | Harvest Server | SC | Root account cracked | No | None Perpetrator Computer Information: HOSTNAME | IP ADDRESS | CITY | STATE | COUNTRY 1. (b) (6), (b) (7)(E).(b) (6), (b) (7)(E) | (b) (6), (b) (7)(E)| Herndon | VA | United States Sensitive Information Involved:No Description of Sensitive Information Involved:None Additional Information:None. NASIRC Action:None. ** -----Original Message----- From: (b) (6), (b) (7)(C) [mailto:(b) (6), (b) (7)(C)ncsa.uiuc.edu] Sent: Tuesday, February 22, 2005 1:24 PM To: nasirc@nasirc.hq.nasa.gov Cc: (b) (6), (b) (7)(C)nasa.gov; (b) (6), (b) (7)(C) Subject: (NASIRC Ref: 107485875) Recent activity Ok folks, here s the latest. Looks like stakkato and crew are back in action. They have been very quite the last few weeks and just recently we started seeing activity again. The stakkato.dyndns.ws address expired on 2/16, but they now have a new trojan. The current host associated with it is a registered domain for someone in Sweden. I am going to wait a bit before we give out the host name until we can find out more info on this person and domain in Sweden (I have already contacted the FBI about it). Here is what is more pertinent to you guys. The following was seen in the log files on the web server we are monitoring: (b) (6), (b) (7)(E) - - [22/Feb/2005:11:14:17 -0500] "GET /openssh-3.7.1p2.tar.gz HTTP/1.0" 200 793332 [tcom-cm-out.jpl.nasa.gov] Can you let me know where they were coming from? I have heard other sites are seeing activity from (b) (6), (b) (7)(E) again. Thanks. (b) (6), (b) (7)(C) Head of Security Operations and Incident Response National Center for Supercomputing Applications Voice : (b) (6), (b) (7)(C) 605 East Springfield Avenue Champaign, IL 61820 Cell : (b) (6), (b) (7)(C) http://www.ncsa.uiuc.edu/(b) (6), (b) (7)(C) Fax : (b) (6), (b) (7)(C) ********************************** ** CLOSED INCIDENTS: 1 *** INCIDENT INFO Incident Name:TCOM-CM-OUT-ID160-02-2005 Discovery Date:22-FEB-05 Exploit Date:22-FEB-05 Labor Hours:14 Labor Cost:1400 HOSTILE SYSTEMS Hostile Name:(b) (6), (b) (7)(E).NYC.RR.COM Hostile IP:(b) (6), (b) (7)(E) AFFECTED SYSTEMS Domain Name:TCOM-CM-OUT.jpl.nasa.gov IP Address:(b) (6), (b) (7)(E) Incident Category:System Compromise Exploit Used:Root account cracked System OS:Sun Solaris 8 (2.8) OS Version:n/a System Security Plan:168 -- *** REVISED CLOSED INCIDENTS: 0 ***
NASIRC Notes:	